# Organisering av informasjonssikkerhet i interkommunale IKT – samarbeid.

*- Særlig om rettslige krav knyttet til sikring av personopplysninger.*


**Av: Lars Haatveit Jenssen**
**Masteroppgave ved Avdeling for forvaltningsinformatikk / juridisk fakultet**
**UNIVERSITETET I OSLO**

# Forord

Informasjons- og kommunikasjonsteknologi (IKT) brukes stadig mer som arbeidsverktøy i kommuner og samfunnet forøvrig. Manuell saksbehandling har i stor grad blitt supplert eller erstattet av elektroniske beslutnings(støtte)-systemer. Innenfor enhver kommune behandles det store mengder personopplysninger. For den enkeltes personvern og den enkeltes tillit til kommunen som tjenesteyter er det viktig at kommunen etterlever sine lovpålagte plikter i forhold til sikring av personopplysninger.

Det er ingen hemmelighet at norske kommuner ofte mangler evnen til å utføre alle sine lovpålagte oppgaver. Dette på grunn av trange budsjett, stor arbeidsmengde og manglende kompetanse. Tanken min har vært at inngåelse av interkommunalt samarbeid om IKT, kan styrke kommuners arbeid med informasjonssikkerhet gjennom kompetanseheving, økte midler og spesialisering. Etter min oppfatning kan inngåelse av interkommunalt IKT-samarbeid gi gevinster i form av bedret informasjonssikkerhet i kommunene som samarbeider. Samtidig vil en nok - ved slikt samarbeid, møte en del utfordringer knyttet til organiseringen og gjennomføring av informasjonssikkerhetsarbeidet. Disse utfordringene bør kanskje også være et signal til blant annet lovgiver, forskriftsmyndighet og Datatilsynet om at det kan være behov for avklaringer og assistanse vedrørende hvordan kommuner på best mulig vis kan samarbeide om ivaretakelse av informasjonssikkerheten.

Arbeidet med denne oppgaven har vært både spennende og lærerikt. Den tar opp temaer og problemstillinger som jeg vet vil engasjere meg også etter at denne oppgaven er levert.

Jeg vil rette en stor takk til Dag Wiese Schartum, Tommy Tranvik og Arild Jansen for veiledning og gode råd. Jeg vil også takke mine kjære venner Sven Ailo Gaup Stadigs og Arngeir Skyttemyr for inspirerende samtaler, kritikk og korrektur.

Denne oppgaven marker slutten på et femårig løp ved Avdeling for forvaltningsinformatikk. Selv om jeg kanskje burde føle meg ferdig nå som jeg leverer, har jeg på følelsen at det er nå det hele begynner.

Oslo, november 2010

Lars Haatveit Jenssen

# Innhold

# Kapittel 1 – Innledning

## 1.1 Bakgrunn for valg av tema

Bruk av informasjons- og kommunikasjonsteknologi (IKT) er svært utbredt i vårt samfunn og veldig mange er avhengige av disse verktøyene i sin arbeidshverdag. Med utstrakt bruk av IKT øker også vår potensielle sårbarhet. Samtidig kan en si at den teknologiske utviklingen også har ført til utvikling av nye og bedre sikkerhetssystemer og rutiner, og at vi kanskje er mindre sårbare i forbindelse med bruk av IKT enn vi var for noen år tilbake. Uansett kan en nok aldri stole 100 prosent på noe IKT- system (Jansen & Schartum 2005:13). Feil bruk av IKT – tilsiktet eller utilsiktet, kan blant annet få konsekvenser for samfunnets stabilitet og sikkerhet, individers integritet og trygghet og/eller organisasjoners og enkeltindividers økonomiske interesser (ibid). Tilstrekkelig sikring av informasjon er derfor svært viktig på mange måter.

I denne oppgaven ser jeg på informasjonssikkerhet i forbindelse med behandling av personopplysninger i et interkommunalt IKT- samarbeid. Årsakene til at jeg har valgt nettopp dette temaet er sammensatte. Blant annet fremkommer det av et brev oversendt fra Datatilsynet til Fornyings og administrasjonsdepartementet (FAD[1]) 31. august 2007 at:

*De offentlige virksomhetene i Norge sitter samlet sett på nærmest ufattelige mengder av informasjon om innbyggerne […] Individet har i liten grad mulighet til å påvirke hvilke former for opplysninger som samles inn og lagres.*

Av denne uttalelsen kan vi forstå at ivaretakelse av informasjonssikkerheten i offentlig sektor berører de fleste borgere og at en tilstrekkelig sikring av personopplysninger er svært viktig for den enkeltes personvern. Dette er kanskje spesielt viktig i kommunal sektor; Avdelingsdirektør i Datatilsynet Leif T. Aanensen har skrevet i en artikkel at: *"Kommunen er, innenfor deler av sin verdiskaping, i en monopolistisk rolle. Innbyggerne kan rett og slett ikke velge bort kommunen som leverandør. Det gjør det desto viktigere at man er seg ansvaret bevisst og ikke utnytter den posisjonen man har."*[2] Den enkelte kommune bør følgelig ta regelverket om informasjonssikkerhet på alvor fordi de gjennom sin myndighetsutøvelse og tjenesteyting behandler opplysninger som er av stor verdi for den enkelte borger, uten at borgeren kan velge bort kommunen som "leverandør".

[1] Nå Fornyings-, administrasjons- og kirkedepartementet
[2] Leif T. Aanensen 2008. Informasjonssikkerhet - et ledelsesansvar

Andre studier – blant annet gjennomført av Transportøkonomisk institutt[3] og Tommy Tranvik[4], viser at kommuner ofte mangler kunnskap og ressurser til å ivareta regelverket vedrørende informasjonssikkerhet. Dette gjelder særlig med hensyn til de organisatoriske tiltakene loven krever iverksatt (Tranvik 2009:99). Videre viser Datatilsynets årsmelding fra 2003 at flere virksomheter de hadde vært hos opplevde regelverket om informasjonssikkerhet som vanskelig å forstå.[5] Det ble også fra flere virksomheter - særlig de små, sagt at de opplevde regelverket som "*for pretensiøst og omfattende for virksomhetens størrelse."*[6]

Det er nok ikke kontroversielt å hevde at mange norske kommuner ofte mangler ressurser og midler til å gjennomføre flere av sine lovpålagte oppgaver. Denne erkjennelsen er en av flere faktorer som ligger til grunn for kommuners ønske om å inngå samarbeid med andre kommuner.[7] For kommuner som mangler kompetanse og personell knyttet til arbeid med informasjonssikkerhet kan kanskje interkommunalt samarbeid være en løsning.

I forarbeidene til endring i kommuneloven vedrørende nye og bedre organisasjonsmodeller for interkommunalt samarbeid,[8] fremgår det at et av de viktigste motivene for inngåelse av interkommunale samarbeid er "*å lage meir kompetente og berekraftige tenesteeiningar […]*". En nærliggende hypotese kan derfor være at inngåelse av et interkommunalt samarbeid om IKT vil styrke informasjonssikkerheten i den forstand at kompetanseheving og spesialisering vil komme hver enkelt kommune til gode. Spørsmålet er om dette faktisk er tilfellet?

Datatilsynet har uttrykt seg positivt når det gjelder inngåelse av interkommunale IKT-samarbeid for å løse utfordringer relatert til behandling av personopplysninger generelt og informasjonssikkerhet spesielt. De har argumentert med at det kan være vanskelig for små kommuner å "*etablere en IT-infrastruktur som ivaretar kommunens behov for fleksibilitet, samtidig som en tilfredsstillende informasjonssikkerhet opprettholdes.*"[9] Med hensyn til de tekniske aspektene ved sikkerhetsarbeidet er det nærliggende å anta at kommunenes evne til å ivareta informasjonssikkerheten vil bedres ved interkommunalt samarbeid om IKT, nettopp på grunn av økt kompetanse og økte ressurser. I dette henseende kan en se for seg at arbeidet

[3] TØI rapport 800/2005
[4] Se Tommy Tranvik sine studier av Informasjonssikkerhet i kommunesektoren i complex 2009.
[5] Datatilsynets årsmelding 2003:17
[6] Datatilsynets årsmelding 2003:17
[7] For mer om ulike motiv for inngåelse av interkommunale samarbeid. Se for eksempel Ot. prp. nr. 95(2005-2006) side 23 flg.
[8] Ot. prp. nr. 95 (2005-2006) Om lov om endringer i lov 25. September 1992 nr 107 om kommuner og fylkeskommuner (interkommunalt samarbeid)
[9] Datatilsynets årsmelding 2003:26

med sikkerhet i forhold til personvern styrkes. Samtidig kan man anta at et slikt samarbeid kan føre til nye typer utfordringer. Kanskje særlig når det gjelder de organisatoriske aspektene. Ved etablering av en samarbeidsorganisasjon skapes nye veier for beslutningstakning og muligens nye hierarkier. Personopplysningsloven med forskrift stiller konkrete krav til virksomheters ledelse og fordeling av ansvar og oppgaver. En tydelig og god organisering anses som en forutsetning for at en skal kunne etterleve lovens krav ellers.

Alle kommuner har et rettslig ansvar for å sørge for tilfredsstillende sikring av de personopplysningene de behandler. Organiseringen av arbeidet skal være forankret hos ledelsen og intern arbeids- og ansvarsdeling skal være klar. Når kommuner inngår et interkommunalt IKT- samarbeid kan en anta at oppgaver som kommunene tidligere har løst alene nå skal løses i fellesskap. Personopplysningsloven § 13 med tilhørende forskrift stiller konkrete krav til organisering, gjennomføring og dokumentasjon av sikkerhetsarbeidet. Når Datatilsynet stiller seg positive til interkommunale IKT- samarbeid presiserer de samtidig at ”[…] *dette stiller store krav til avklaring av ansvarsforhold og en dokumentert informasjonssikkerhet.*”[10] Denne type avklaringer er selvfølgelig sentrale når en kommune ”jobber alene”, men trolig vil avklaring av ansvars- og myndighetsforhold fremstå som desto viktigere når man er flere som skal løse oppgaver i fellesskap. Lovens bestemmelser gjelder ikke interkommunale samarbeid direkte og dermed kan det bli vanskeligere å anvende loven og forskriften på slike tilfeller. Det er derfor grunn til å være ekstra oppmerksom på lovens regler når en samarbeider med andre kommuner om informasjonssikkerhet.

[10] Datatilsynets årsmelding 2003:24

## 1.2 Problemstilling og avgrensning

Temaet for denne oppgaven er hvorvidt kommuners inngåelse av interkommunalt IKT-samarbeid påvirker deltakerkommunenes organisering av arbeid med sikring av personopplysninger. Personopplysningslovens § 13 og tilhørende forskrift kapittel 2 krever at informasjonssikkerheten skal være *tilfredsstillende* og at dette skal oppnås gjennom planlagte og systematiske tiltak. Typen og mengden tiltak kan være mange; organisatoriske, teknologiske, bygningstekniske, personalmessige, pedagogiske, rettslige og økonomiske (se f.eks. Tranvik 2009:21 og Haug 2006:16). Poenget er at lovgivningen forutsetter at ulike virkemidler blir tatt i bruk for å oppnå dens krav. Haug gir et eksempel: "*Hvis reglene […] sier at uvedkommende ikke skal få tilgang til konfidensiell informasjon, kan dette forutsette bl.a. fysiske og tekniske, organisatoriske og pedagogiske virkemidler."* (Haug 2006:17). Følgelig forstår vi at arbeidet med informasjonssikkerhet er omfattende. Jeg har imidlertid valgt å fokusere på de organisatoriske aspektene ved informasjonssikkerhet.

Ved studier av informasjonssikkerhet kommer en ikke utenom teknologi. Loven, og forskriften spesielt, har særlig fokus på elektronisk behandling av personopplysninger. Implisitt forstår vi derfor at teknologien spiller en viktig rolle. Likevel stiller ikke loven eller forskriften konkrete krav til valg av tekniske sikkerhetsløsninger. Det er i utgangspunktet den enkelte kommune (eller annen type virksomhet) som selv må utrede og avgjøre ønsket grad av teknisk sikkerhet. På den annen side er det ikke særlig tvil om at en må besitte en viss teknologisk kompetanse for å gjennomføre en del av de tiltakene loven og forskriften lister.

Organisatoriske forhold er mer omfattende regulert i regelverket. Det stilles spesifikke krav til organisering; avklaring av ansvars- og myndighetsforhold, opprettelse av sikkerhetsorganisasjon, gjennomføring av risikovurderinger etc. Det er denne type forhold som skal drøftes i lys av interkommunalt IKT- samarbeid.

Hvorvidt samarbeidsordningen fører til at kommunene og samarbeidet faktisk møter lovens krav om tilfredsstillende informasjonssikkerhet er et annet spørsmål, et som jeg ikke skal ta for meg her. Dette begrunnes blant annet i at kommuner ikke har lov til å utlevere dokumenter gjeldene risikovurderinger, sikkerhetstiltak og trusler jf. personopplysningsforskriften § 2-11. Derfor vil jeg ikke ha godt nok grunnlag for å si noe om en kommunes informasjonssikkerhet faktisk er tilfredsstillende. Det en derimot kan si noe om er hvorvidt forholdende ligger til rette for at tilfredsstillende sikkerhet kan oppnås.

En annen årsak til at det er de organisatoriske forholdene som vil være mitt fokus er uttalelser fra blant andre Datatilsynet, foreningen Kommunal informasjonssikkerhet (KINS[11]) og Kommunesektorens interesse- og arbeidsgiverorganisasjon (KS) som alle tyder på at det er i forhold til de organisatoriske aspektene at ivaretakelse av informasjonssikkerhet skorter mest.

Dersom organisering av sikkerhetsarbeidet i den enkelte kommune blir sett på som en utfordring i seg selv, kan en tenke seg at kommuner som samarbeider om prosesser som innebærer elektronisk behandling av personopplysninger tilføyer problematikken en ny dimensjon. På hvilken måte vil kommuners inngåelse av interkommunalt IKT- samarbeid påvirke deres organisering av sikkerhetsarbeidet? Hvordan vil ansvars- og myndighetsforholdene endres?

På bakgrunn av disse tankene starter jeg med følgende spørsmål:

1. Hvordan er de rettslige ansvars- og myndighetsforholdene fordelt mellom deltakerkommunene og organet for det interkommunale IKT- samarbeidet?

    a. I hvilken grad er disse forholdene dokumentert?
    b. I hvilken grad er disse forholdene i samsvar med lov og forskrift?

Ut i fra en hypotese om at inngåelse av et interkommunalt IKT- samarbeid er med på å endre organiseringen av kommunenes arbeid med IKT, kan det være naturlig å se på hvorvidt ansvars- og myndighetsforhold også endres. Når en kombinerer denne antagelsen med tidligere forskning som viser at kvaliteten på sikkerhetsdokumentasjon i kommune- Norge ikke alltid er like god,[12] oppstår det også et spørsmål om i hvilken grad reguleringen av ansvar og myndighet hos deltakerkommunene og samarbeidsorganisasjonen er i samsvar med lov og forskrift. Etter å ha undersøkt disse forholdene vil jeg videre se på det ansvaret som ligger hos

[11] Leder i KINS- Stein Fotland, har ved flere anledninger henvist til *Paretos lov* ved presentasjoner av utfordringene relatert til informasjonssikkerhet. Han hevder at ivaretakelse av informasjonssikkerhet består 20 % av tekniske aspekter og 80 % prosent av holdninger (herunder organisering av arbeidet).

[12] Se bl.a. ENISA sin undersøkelse: Security Awareness Management in local Governments: Approaches in Scandinavia (tilgjengelig på http://www.enisa.europa.eu/act/ar/deliverables/2008/scandinavian-approaches-survey). Se også Tranvik 2009. Han viser at kravene til sikkerhetsdokumentasjon etterleves i større grad enn bestemmelser om organisering og gjennomføring av sikkerhetsarbeidet, men at det finnes en del mangler i norske kommuners sikkerhetsdokumentasjon også. Særlig når det gjelder akseptkriterier og rutiner for risikovurderinger (Tranvik 2009:77).

den enkelte aktør og hvorvidt de oppgavene den enkelte har blitt pålagt blir gjennomført i praksis.

2. I hvilken grad er den dokumenterte ansvars- og myndighetsfordelingen ivaretatt i praksis?
    a. Utfører de ulike aktørene de oppgaver de er pålagt etter avtalen mellom de samarbeidende kommunene?
    b. I hvilken grad er de oppgavene som gjennomføres i tråd med loven?

Tidligere forskning indikerer at dokumentasjon knyttet til informasjonssikkerhetsarbeidet i norske kommuner ikke alltid stemmer overens med praksis.[13] Med dette som utgangspunkt ønsker jeg å få klarhet i om de ansvarsforholdene som er dokumentert og de rollene som er tildelt faktisk er i tråd med føringene i lov og forskrift, og om de oppgavene som er tildelt ulike personer i deltakerkommunene og samarbeidsorganisasjonen faktisk blir gjennomført.

Etter å ha besvart spørsmål 1 og 2 bør jeg ha et rimelig klart bilde av de organisatoriske ordningene, oversikt over arbeidsoppgaver og et inntrykk av hvorvidt forholdene ligger til rette for en tilfredsstillende organisering av informasjonssikkerhetsarbeidet. Jeg vil trolig også ha et grunnlag for å si noe om;

3. I hvilken grad den interkommunale samarbeidsorganisasjonen påvirker informasjonssikkerhetsarbeidet i den enkelte kommune.
    a. Om samarbeidet har endret kommunenes arbeid med informasjonssikkerhet på noen måte, eller om alt er som før?
    b. Om inngåelsen av interkommunalt IKT – samarbeid styrker den enkelte kommunes ivaretakelse av informasjonssikkerhet knyttet til behandling av personopplysninger?

Min hypotese er at inngåelse av interkommunalt samarbeid kan bidra til økt kompetanse, økt kunnskap og en større økonomisk handlekraft. Når det samarbeides om IKT er det også spennende å se på om den antatte økte kompetansen og kunnskapen gir noen gevinst i form av bedret arbeid med informasjonssikkerhet eller ikke. Det er i alle fall rimelig å anta at de

[13] Se bl.a. ”Personvern og informasjonssikkerhet” av Tommy Tranvik og diskusjonene rundt ”etterlevelsesillusjonen”.

endringene i organisasjonsstrukturen - som et omfattende samarbeid om IKT antas å kreve, vil påvirke deltakerkommunenes informasjonssikkerhetsarbeid på en eller annen måte.

Av problemstillingen forstår man at dette ikke er en ren rettsdogmatisk oppgave. Jeg tar også opp temaer som kan sies å ligge nærmere organisasjonsteori enn jus. På samme tid krever en oppgave som denne at man diskuterer informasjonssikkerhetens teknologiske aspekter. Oppgaven får dermed et tverrfaglig tilsnitt. Dette kan igjen gi en pekepinn på at informasjonssikkerhetsarbeid er utfordrende og at et kriterium for oppnåelse av tilfredsstillende informasjonssikkerhet er en kombinasjon av god juridisk, teknologisk og organisatorisk forståelse. Dermed kan en argumentere for at en studie som denne er avhengig av diskusjoner innenfor alle de tre overnevnte perspektivene, for å få frem et en helhetlig forståelse av de utfordringene kommuner står ovenfor ved planlegging og gjennomføring av informasjonssikkerhetsarbeid.

## 1.3 Presentasjon av det interkommunale IKT- samarbeidet (caset)

### 1.3.1 Kort om kommunesektoren i Norge

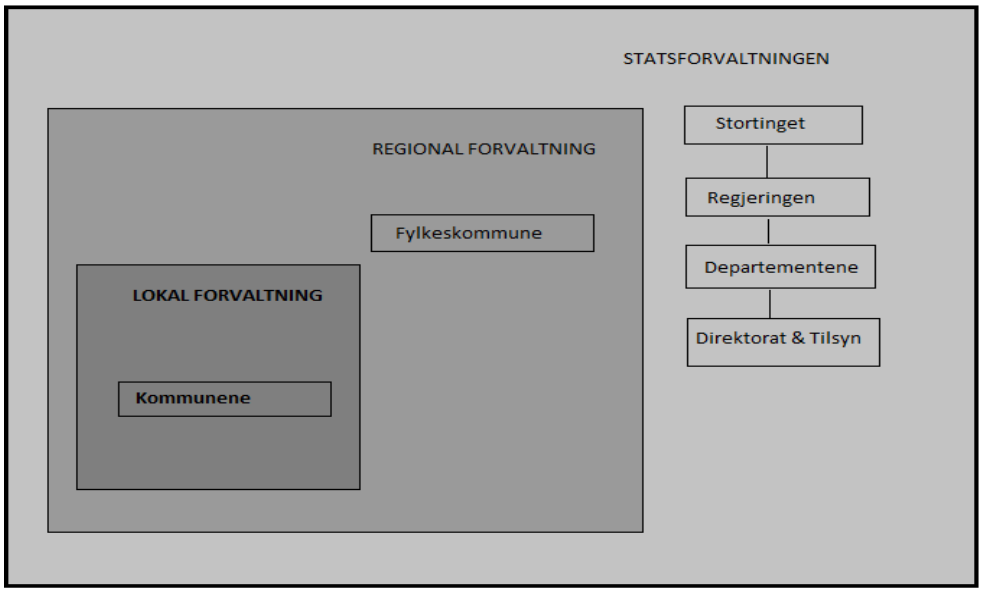
I denne oppgaven behandles informasjonssikkerhet i lys av kommuner og interkommunalt samarbeid. Av den grunn er det nødvendig å si litt om den norske kommunesektoren og litt om interkommunale samarbeid.

En kommune betegner et geografisk avgrenset område og utgjør en egen politisk og administrativ enhet innenfor staten. I dag er det 430 kommuner i Norge (2010).[14] Kommunene utgjør det nederste nivået i det norske styringssystemet etter statsforvaltningen og fylkeskommunene.

At kommunene er på det nederste nivået innebærer også at de er det myndighetsorganet som er nærmest borgeren. Kommunene spiller en viktig rolle i det norske samfunnet og er i første rekke ansvarlig for sine egne innbyggeres grunnleggende velferdsgoder som skolegang, sosialhjelp, barnehageplasser, barnevern og kommunal legetjeneste. Det er ingen tvil om at store mengder personopplysninger blir behandlet når en kommune utøver disse oppgavene for borgerne. De nevnte ansvarsområdene er alle lovfestede oppgaver som kommunene er pålagt av Stortinget å utføre.  Kommuner (og fylkeskommuner) er ikke del av den hierarkisk ordnede statsforvaltningen (jf. figur 2). De er ikke underlagt staten og er dermed ikke underlagt

[14]Kommunal- og regionaldepartementet http://www.regjeringen.no/nb/dep/krd/tema/forholdet-kommune-stat/fakta-om-kommunene-og-fylkeskommunene.html?id=548623 (lest 13.4.2010)

regjeringens instruksjons- og organisasjonsmyndighet. Kommuner styres derfor gjennom lovgivning (Bernt et. al 2002:23, Fimreite & Grindheim 2007:119).




**Figur 1. Oversikt over forvaltningsnivåene i Norge. Kommuner og fylkeskommuner er adskilt fra statsforvaltningen og styres i utgangspunktet kun av stortinget som lovgiver. Figuren er hentet fra www.norge.no**

Tall fra Kommunal og regionaldepartementet peker på at den norske kommunestrukturen kjennetegnes av mange kommuner med få innbyggere.[15] Tall fra 1. januar 2006 viser at 54 % av norske kommuner har under 5000 innbyggere og at tre av fire norske kommuner har under 10 000 innbyggere.[16] Det at det er så mange små kommuner er med på å gjøre at diskusjonen om kommunesammenslåing ligger latent og at den ved jevne mellomrom kommer opp i samfunnsdebatten. Til tross for utredninger[17] og annen debatt på feltet[18] ble det besluttet av Stortinget 1. juni 1995 at ingen kommuner skulle slås sammen i mot deres vilje (Fimreite og Grindheim 2007:124).[19] I fravær av reformer med sikte på ytterligere kommunesammenslåing, har kommunalt og interkommunalt samarbeid fremstått som en løsning på noen av utfordringene.

[15] St.meld. nr. 12 (2006-2007) Kapittel 9.
[16] Ibid. (se figur 9.1)
[17] For eksempel utredning forfattet av Christiansen-utvalget. Se for øvrig NOU 1992:15
[18] Denne debatten ble nylig tema i magasinet Juristkontakt (nr. 2- 2010) hvor det vises til en undersøkelse utført av juristforbundet som har kartlagt jurister i kommune-Norge. Det kommer frem at bare en av tre kommuner har en jurist ansatt og at dette funnet viser at rettsikkerheten til borgerne i den enkelte kommune ofte kan være truet. Som en kommentar til denne undersøkelsen sier Akademikernes leder Knut Aarbakke til Dagens Næringsliv at dette igjen aktualiserer debatten om kommuneslåing fordi det er vanskelig for, særlig små kommuner, å ansette jurister og andre akademikere. Han tar på bakgrunn av dette til orde for tvangssammenslåing av kommuner.
[19] St.meld. nr. 12 (2006-2007) avsnitt 9.2.1 - Frivillighetsprinsippet

### 1.3.2 Kort om interkommunale samarbeid.

Ovenfor har jeg kort vært innom debatten om kommunesammenslåing og nevnte i den forbindelse at inngåelse av interkommunalt samarbeid kan ses på som et slags alternativ til kommunesammenslåing. Sentralt i debatten om kommunesammenslåing står faktorer som kommunalt selvstyre og lokal ekspertise på den ene siden og ønsket om effektivitet og stordriftsfordeler på den andre. Som vi har sett er debatten om ytterligere store kommunesammenslåinger foreløpig tonet ned. Ønsket om stordriftsfordeler og økt effektivitet kan i utgangspunktet likevel realiseres, uten at det nødvendigvis går på bekostning av det lokale selvstyret i den grad det muligens ville gjort ved kommunesammenslåing. Dette kan oppnås med interkommunalt samarbeid. I forarbeidene til lov om endringer i kommuneloven blir ønsket om økt kompetanse, effektivitet og kostnadseffektivitet løftet frem som hovedårsaker til inngåelse av kommunale samarbeidsordninger.[20] Samtidig sies det at ønsket om å inngå slikt samarbeid sjeldent begrunnes i at en vil unngå kommunesammenslåing og/eller et ønske om å legge til rette for sammenslåing. Til tross for dette kan en møte en del av kritikken rettet mot mangelen på kompetanse og kostnadseffektivitet - særlig på grunn av antallet små kommuner, ved å inngå samarbeid med andre kommuner.

I 2006 kartla konsulentselskapet ECON omfanget av interkommunale samarbeid i Norge på vegne av KS.[21] Kun 158 kommuner besvarte spørsmålene i undersøkelsen. Blant disse kom det frem at hver kommune var del av mellom 8 og 21 samarbeidsordninger, dette utgjorde totalt 1417 unike samarbeid.[22] Tallet ville naturligvis vært større, om flere kommuner hadde svart. I 2008 var det mellom 35-40 interkommunale samarbeid direkte myntet på samarbeid om IKT.[23] Samarbeid innenfor dette feltet har hatt særlig vekst det siste tiåret (Lanestedt 2008:19).

Interkommunale samarbeid kan organiseres på flere måter; som et interkommunalt styre etter kommuneloven §§ 27 og/eller 28, interkommunale selskaper etter IKS –loven,[24] som aksjeselskaper etter lov om aksjeselskaper,[25] stiftelser eller mer eller mindre forpliktende enkeltavtaler mellom kommunene. Hagen og Sørensen peker på at erfaringene med interkommunalt samarbeid er av varierende suksess (Hagen & Sørensen 2006:110). De

[20] Ot.prp. nr 95 (2005-2006)
[21] ECON rapport 2006-057
[22] KS – ”all makt i denne sal” 2006.
[23] På nettsiden www.ksikt.no finner man en oversikt over noen av disse samarbeidene
[24] lov om interkommunale selskaper (lov 29. januar 1999 nr. 6)
[25] lov om aksjeselskaper (lov 13.juni 1997 nr. 44)

hevder at samarbeidene ofte ikke har hatt den ønskede stabiliteten og varigheten man i utgangspunktet hadde ønsket seg. Dette har vært særlig fremtredende i samarbeid bestående av mange små kommuner, i motsetning til samarbeid der en av kommunene har vært stor. I forhold til samarbeid om IKT blir små kommuners vilje til å samarbeide med større kommuner nærmest nødvendig for at de skal kunne holde tritt med utviklingen av teknologi og borgeres krav til digitale tjenester (Lanestedt 2008:21). Vi skal se at sistnevnte poeng har vært en viktig forutsetning for IKT- samarbeidet som studeres i denne oppgaven.

### 1.3.3 Spesielt om caset

Ved valg av hvilket interkommunalt IKT- samarbeid jeg skulle fordype meg i var det særlig to kriterier som var viktige. 1) Samarbeidet måtte ha vært etablert en stund. Dette begrunnes i at eventuelle barnesykdommer var blitt håndtert og at samarbeidet skulle ha fått "satt seg". 2) Samarbeidet skulle ha en viss geografisk nærhet til Oslo slik at jeg ville ha mulighet til å foreta intervjuer ansikt til ansikt uten at dette krevde for mye reisetid.

Det interkommunale IKT- samarbeidet som studeres i denne oppgaven er organisert som et interkommunalt styre etter kommunelovens § 27. Denne organiseringen er en av de mest utbredte modellene for interkommunalt samarbeid. Samarbeidet består av fire kommuner. Kommune 1 er med sine omlag 60 000 innbyggere å betrakte som en storkommune.[26] Mens de øvrige kommunene (2, 3 og 4) med henholdsvis omlag 6 000, 8 000 og 18 000 innbyggere regnes som mellomstore kommuner. Samarbeidet ble opprettet i 2004, men kommune 4 tiltrådte ikke samarbeidet før 1. januar 2010.

Hensikten med etableringen av samarbeidet var å jobbe sammen om IKT. De forskjellige kommunene hadde noe ulike behov og motiv, men alle deltakerne mente de hadde noe å vinne på inngåelse av samarbeid og ideen om interkommunalt samarbeid var en uttalt politisk strategi hos alle kommunene. I kommune 1 var motivet et ønske om å være en sentral aktør for regional utvikling, i tillegg til at opprettelsen av et slikt samarbeid antageligvis ville styrke IKT- utviklingen i kommunen. For kommune 4 var det muligheten for å oppnå en bedre nærhet mellom IKT- tjenesten og egen organisasjon som var hovedmotivasjonen. Både bruk av eksterne leverandører og eget arbeid med utvikling, kunne erstattes med en ny interkommunal samarbeidsorganisasjon. Hos kommune 2 og 3 var begrunnelsen for samarbeidet først og fremst behovet for å styrke sin IKT- funksjon, med særlig vekt på

[26] SSB rangerer kommuner som små (færre enn 5 000 innbyggere), mellomstore(fra 5 000 til 19 999 innbyggere) og store (20 000 innbyggere oppover).

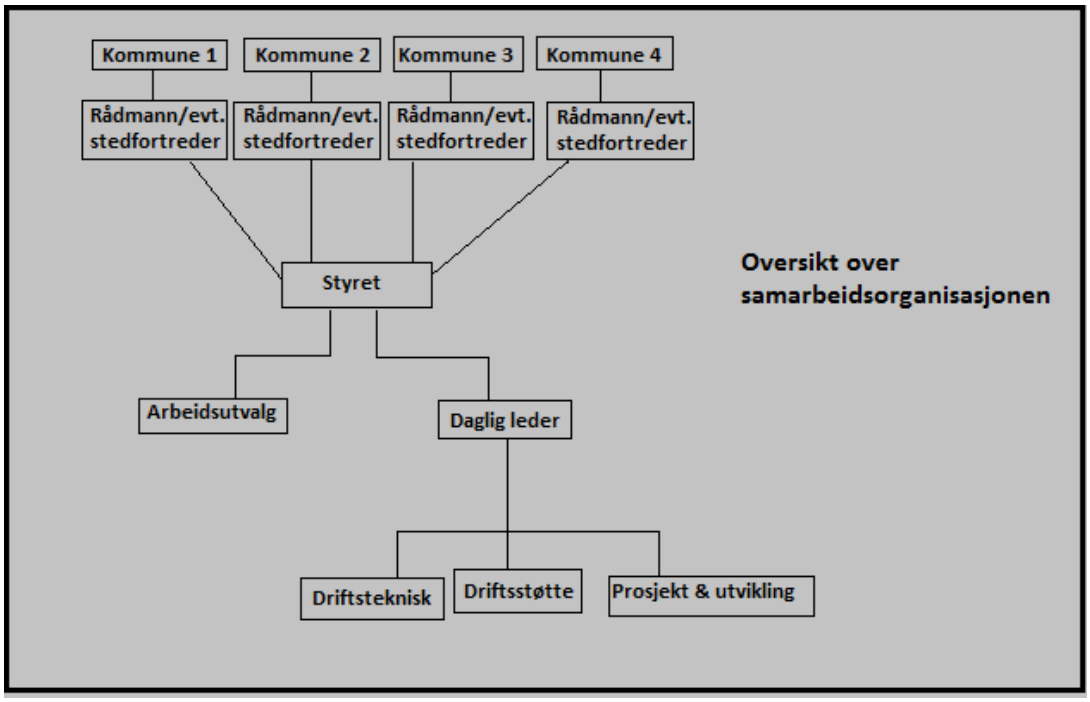
planlegging og utvikling. Samtidig hadde begge disse kommunene meget begrenset bemanning når det gjaldt drift og brukerstøtte. Dette gjorde at deres IKT- systemer var mer sårbare enn hva en ønsket og det hemmet deres muligheter for å bygge opp og vedlikeholde IKT- kompetanse i sine respektive kommuner. Rapporten som ble utarbeidet vedrørende mulighetene for etablering av samarbeidet viser til en felles erkjennelse blant kommunene om at IKT er en virksomhetskritisk ressurs og alle kommunene vil møte økende krav til og forventninger knyttet til sine IKT- systemer.[27] Som vi så i avsnitt 1.3.2 kan erfaring tyde på at det å ha med en storkommune er en viktig forutsetning for å lykkes med interkommunalt samarbeid. Respondentene jeg har snakket med i denne oppgaven har alle trukket frem kommune 1 sin størrelse og deres ressurser som viktig. Det er kommune 1 som har vært pådriver og som har bidratt til at samarbeidsorganisasjonen i dag fremstår som en profesjonalisert IKT- avdeling.

Det er viktig å presisere at samarbeidet som studeres her ikke er et rent samarbeid om informasjonssikkerhet, men i hovedsak et samarbeid om felles drift, infrastruktur og innkjøpsavtaler. Totalt sett behandles store mengder personopplysninger i deltakerkommunene. Kommuner er komplekse organisasjoner med mange virksomhetsområder. Innenfor disse virksomhetsområdene behandles det ofte svært mange personopplysninger. Det være seg virksomheter innenfor skole og utdanning, sykehjem og hjemmehjelp, barnevernstjenester og kommunelege etc. Så informasjonssikkerhet og de utfordringene som kan relateres til ivaretakelse av denne er absolutt et tema deltakerne bør ha kunnskap om og fokus på. I prosjektrapporten ble det anbefalt at felles retningslinjer for sikkerhet skulle etableres.[28] Dette kan være et godt tiltak. For selv om kommuner kan virke intrikate med mange ulike instanser som behandler personopplysninger, så har alle kommuner samme type oppgaver og samme type regelverk og forholde seg til. Dette er nok med på å gjøre at samarbeid fremstår som en farbar vei. I brevet fra Datatilsynet til FAD som jeg viste til i avsnitt 1.1. ble viktigheten av fokus på informasjonssikkerhet i offentlig og kommunal sektor begrunnet i de store og ulike mengdene personopplysninger som behandles der. Det interkommunale IKT- samarbeidet som blir studert i denne oppgaven har til sammen ca 95 000 innbyggere, 10 000 datamaskiner og 5000 personer som kan logge seg på datamaskiner og systemer som organisasjonen drifter. Opparbeidelse av et godt regime for sikring av personopplysninger blir derfor svært viktig, men kanskje også svært utfordrende.

[27] Prosjektrapport: Etablering av interkommunal IKT- tjeneste for kommune 1,2,3 og 4. 2005.
[28] Ibid.

En skal huske på at hver kommune har et rettslig ansvar for sikring av de personopplysninger de selv behandler, selv om de er med i et interkommunalt samarbeid.

Kommunelovens § 27 er en forholdsvis åpen bestemmelse i den forstand at den ikke stiller for mange spesifikke krav til organisering. Kravene som stilles er at samarbeid etablert etter bestemmelsen ikke kan drive myndighetsutøvelse. Samarbeidet som studeres her har definert IKT som et administrativt anliggende og driver således ikke myndighetsutøvelse i sin organisasjon. Alle beslutninger som inneholder elementer av myndighetsutøvelse, må eventuelt godkjennes av deltakerkommunenes kommunestyrer. Ellers kreves det at et samarbeid etter denne hjemmelen skal ha egne vedtekter. Disse skal inneholde styrets sammensetning, hvordan det utpekes og området for styrets virksomhet jf § 27 nr. 2, bokstav a og b. Av økonomiske faktorer skal vedtektene inneholde bestemmelser om hvorvidt deltakerkommunene skal gjøre innskudd til virksomheten og om styret har myndighet til å ta opp lån eller på annen måte pådra deltakerne økonomiske forpliktelser jf bokstavene c og d. Siste krav vedrørende vedtektenes innhold gjelder uttreden fra eller oppløsning av samarbeidet jf. kommuneloven § 27 nr. 2, bokstav e. Etter vedtektene har det interkommunale samarbeidet definert seg selv som et eget rettssubjekt. Et organisasjonskart for IKT – samarbeidet viser sammensetningen og relasjonene.




**Figur 2. Organisasjonskart over samarbeidsorganisasjonen**

Organisasjonen har et eget styre som utgjør den øverste ledelsen. Styret har det organisatoriske og administrative ansvaret for driften av samarbeidet. Under styret er det et arbeidsutvalg som skal være et "koordinerende organ" for deltakerkommunene og som har en rådgivende funksjon i forhold til styret. [29] Samarbeidet har i tillegg en daglig leder med ansvar for den daglige administrative og faglige driften av samarbeidet.

Styret har fire medlemmer. Disse er rådmennene fra den enkelte kommune eller den han/hun oppnevner som sin stedfortreder. Alle kommunene har lik stemmevekt i styret. Lederen av styret skal etter vedtektene være representanten fra kommune 1. Per dags dato er det assisterende rådmann i kommune 1 som er styreleder. Det skal avholdes styremøter minimum to ganger i året.[30] I følge vedtektene er styret beslutningsdyktig når kommune 1 og en representant fra én annen kommune er representert. Styrets oppgaver er ellers å vedta økonomiplan, budsjett, virksomhetsplan, regnskap og årsmelding. Budsjettet kan likevel ikke anses som gyldig før det er godkjent av det enkelte kommunestyre. Etter vedtektene kan styret delegere myndighet til arbeidsutvalget og daglig leder. Styrets instruksjonsmyndighet betegnes som ubegrenset.

[29] Organisasjonens vedtekter
[30] I følge vedtektene kan styrets leder eller kalle inn til møte når han finner det nødvendig eller når minst ett av styrets medlemmer krever det.

Arbeidsutvalget består av fire medlemmer. Dette skal være personer som er tillagt det utøvende ansvar for IKT funksjonen i den enkelte deltakerkommunen. Arbeidsutvalget kan ses på som bindeleddet mellom den enkelte kommune og IKT- tjenesten.

Den daglige lederen har det daglige ansvaret for den løpende drift av samarbeidet og er underlagt styret, hvor han også har møte- og talerett.  Det er styret - etter nærmere avtale med kommune 1, som utpeker den daglige lederen og fastsetter vilkår og retningslinjer for denne.

Organisasjonen har per i dag omlag 40 ansatte og hadde i 2009 et driftsbudsjett på 40,5 millioner kroner. Organisasjonen har lokaler i rådhuset til kommune 1 og består av tre avdelinger: driftsteknisk, driftsstøtte og ”prosjekt og utvikling”.

## 1.4 Kort om rettslige krav til sikring av personopplysninger

"Informasjonssikkerhet" er et vidt begrep med iboende juridiske, teknologiske og organisatoriske perspektiver. Da de vurderingene rundt informasjonssikkerhet som gjøres i denne oppgaven i hovedsak er basert på reguleringene i personopplysningsloven med forskrift, vil jeg innledningsvis knytte noen ord til denne lovgivningen.

### 1.4.1 Om personopplysningsloven

Den sentrale loven i denne oppgaven er lov om behandling av personopplysninger (lov av 14. april 2000 nr.31), heretter forkortet pol. Denne avløste personregisterloven av 1978. Til forskjell fra personregisterloven, har pol mindre fokus på personregistre og i stedet generelt fokus på elektronisk behandling av personopplysninger. For at en skal kunne tilfredsstille lovens krav til sikring av personopplysninger forutsettes det at det ellers skjer en lovlig behandling av personopplysninger.

Formålet med pol er:

*[…] å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.* [31]

Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn. I dette ligger den enkeltes behov for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.[32]

Med personopplysninger menes alle *opplysninger og vurderinger som kan knyttes opp til en enkeltperson*, se pol § 2, nr. 1. Dette er en vid definisjon og regelverket gjelder for kommunal, statlig og privat sektor (Schartum 20005:98). Pol § 3 bokstav a og b fastsetter lovens saklige virkeområde. Her angis det at loven gjelder for behandling av personopplysninger som skjer helt eller delvis ved bruk av elektroniske hjelpemidler og også annen behandling av personopplysninger når disse er eller skal bli del av et personregister.[33]

[31] Jf. pol § 1
[32] jf. pol § 1
[33] Når det gjelder det saklige virkeområdet må det presiseres at loven ikke gjelder for behandling av personopplysninger til rent private eller personlige formål jf. pol § 3 annet ledd. I tillegg finnes det unntak i pol § 7 som regulerer lovens forhold til ytringsfriheten. I dette henseende gjelder kun en begrenset del av loven med tanke på behandlinger gjort som ledd i kunstneriske, litterære eller journalistiske formål.

For at en skal kunne behandle personopplysninger må man ha et rettslig grunnlag, se pol §§ 8 og 9.[34] Pol § 11 inneholder videre det som blir betegnet som "grunnkrav" til behandling av personopplysninger. Her finner vi en påminnelse om at §§ 8 og 9 må være oppfylt, samtidig som den angir krav til formål for behandling under bokstavene b og c og at opplysningene skal være tilstrekkelige, relevante, korrekte og oppdaterte.[35] Opplysningene skal heller ikke lagres lengre enn nødvendig, jf. bokstavene d og e.

### 1.4.2 Om sikring av personopplysninger jf. pol § 13 og personopplysningsforskriften kapittel 2

Det er pol § 13 som regulerer spørsmål om informasjonssikkerhet.

I bestemmelsens første ledd heter det at det er den behandlingsansvarlige (den som bestemmer formålet med behandlingen og de hjelpemidler som skal brukes jf. pol § 2, nr 4) og en eventuell databehandler (den som behandler personopplysninger på vegne av den behandlingsansvarlige jf. pol § 2, nr 5) som skal påse at personopplysningene sikres på en tilfredsstillende måte. Det som skal beskyttes er de ulike opplysningenes behov for *konfidensialitet, integritet* og *tilgjengelighet*.

Med ***konfidensialitet*** menes det at personopplysninger ikke skal gjøres kjent for andre enn de som har autorisert/tjenestelig tilgang til dem (Johansen et. al 2001:353). Dette innebærer at en må sette opp sikkerhetstiltak som gjør at uvedkommende ikke får innsyn, men også at de som har innsyn ikke misbruker dette. Med personopplysningers ***integritet*** menes det at opplysningene skal beskyttes mot uautorisert endring (Johansen et. al 2001:344). I dette ligger det at kun de med fullmakt til å endre opplysningene kan gjøre det, og i tillegg skal operasjonene disse personene utfører i informasjonssystemet logges. Med ***tilgjengelighet*** menes det at tilstrekkelige og relevante personopplysninger skal være tilgjengelige når det er nødvendig (Johansen et. al 2001:344).

Sikringen av personopplysningene skal skje gjennom ***planlagte og systematiske tiltak***. Med bruk av denne formuleringen kan en tenke seg at lovgiver peker mot en metodisk tilnærming. Denne tilnærmingen er nærmere beskrevet i forskriftens kapittel 2 som er hjemlet i pol § 13 siste ledd:

[34] Pol § 8 angir vilkår for å behandle personopplysninger. En behandling er kun lovlig dersom den registrerte samtykker, det er fastsatt i lov eller dersom behandlingen er nødvendig ut i fra visse kriterier jf § 8 bokstavene a-f. Pol § 9 regulerer særlig sensitive opplysninger. Slike opplysninger kan kun behandles dersom et av vilkårene i § 8 er oppfylt sammen med et av vilkårene i § 9 bokstavene a-h.
[35] Schartum og Bygrave 2006:81.

*Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak.*

Denne bestemmelsen viser til forskrift av 15. desember 2000 nr 1265 om behandling av personopplysninger (heretter: pof.). Før videre redegjørelse av forskriften presiserer jeg at det er pol § 13 som utgjør rammene for hva som kan bestemmes i forskrift. I og med at pol § 13 kun krever tilfredsstillende sikkerhet, kan en vanskelig sette helt bestemte krav i forskriften til hvilke tiltak den enkelte behandlingsansvarlige og databehandler skal iverksette. Ved å bruke ordet *skal* i flere av sine bestemmelser, gir forskriften uttrykk for at slike bestemmelser er obligatoriske. Av læren om reglers trinnhøyde må en forstå det slik at det ikke foreligger noen rettslig plikt til å gjennomføre tiltakene i forskriften dersom de ikke anses å være nødvendige for å oppnå tilfredsstillende sikkerhet etter pol § 13 (Schartum 2005:118). I praksis kan det likevel være at de fleste av kravene i forskriften må anses som nødvendige. Derfor bør den behandlingsansvarlige og en eventuell databehandler vurdere alle kravene i forskriften nøye (ibid.) og dersom noen av tiltakene vurderes som unødvendige, bør disse konklusjonene begrunnes.

Det er forskriftens kapittel 2 som legger videre føringer på hvordan en skal tilnærme seg arbeidet med sikring av personopplysninger. I avsnitt 1.4.1 så vi at pol § 3 angir lovens saklige virkeområde og at dette innebefatter helt eller delvis elektroniske behandlinger, samt manuelle behandlinger av personopplysninger. I pof § 2-1 – som angir forholdsmessige krav til informasjonssikkerhet, er det kun snakk om behandlinger som skjer helt eller delvis elektronisk. Manuelle behandlinger faller derfor utenfor bestemmelsene i forskriften.[36] På lik linje med pol § 13 angir pof § 2-1 viktigheten av å beskytte personopplysninger og herunder deres behov for konfidensialitet, integritet og tilgjengelighet. Bestemmelsens andre ledd presiserer også at kravene til sikring av personopplysninger skal være forholdsmessige. I dette ligger det at tiltak som gjelder sikring av personopplysninger skal stå i forhold til sannsynligheten for sikkerhetsbrudd og eventuelle konsekvenser av slike brudd (Johansen et al. 2001:346).

Når det gjelder den praktiske ivaretakelsen av pol § 13 og pof kapittel 2 kan en særlig støtte seg til to prinsipper: Risikostyring og ledelsesstyring.

[36] For manuelle behandlinger gjelder likevel de generelle kravene til informasjonssikkerhet etter pol § 13.

Risikostyring handler om at man skal forsøke å forutse og redusere risikoen for at potensielle uønskede hendelser skal ramme personopplysningers behov for konfidensialitet, integritet og tilgjengelighet (Tranvik 2009:90). Slay og Koronios understreker at risikostyring (risk management) er en kontinuerlig prosess der en stadig skal vurdere sannsynligheten for at uønskede hendelser skal inntreffe (Slay & Koronios 2006:2). Av dette må man forstå at arbeid med risikostyring ikke er noe man gjør én gang, men at det er en "løpende" prosess å evaluere risiko.

Ideen om en risikostyrt tilnærming til sikkerhetsarbeidet kan relateres til lovens bruk av "tilfredsstillende informasjonssikkerhet" jf. pol § 13, 1. ledd og videre lovens og forskriftens krav om planlagte og systematiske tiltak jf. pol § 13, 1. ledd og pof § 2-1. Med *tilfredsstillende* må vi forstå at kravene i loven er forholdsmessige. Dette presiseres også i pof § 2-1. Forutsetningen om forholdsmessighet er tatt inn i bestemmelsen med tanke på ulike virksomheters størrelse og verdien av den informasjon de behandler og skal beskytte. Det er ikke snakk om å fjerne risikoen helt, men det handler om å fastlegge hva som er akseptabel risiko for den aktuelle virksomhet.

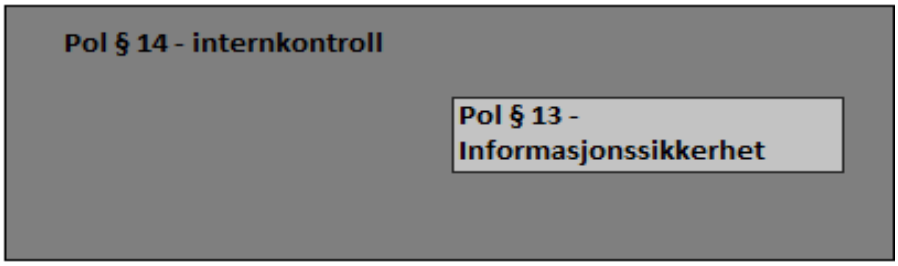
Med ledelsesstyring menes at sikringsarbeidet skal forankres hos den øverste ledelsen i virksomheten. I en kommune vil dette normalt bety rådmannen eller rådmannsapparatet. En forstår således at forskriftsmyndigheten har lagt opp til at den øverste ledelsen skal styre arbeidet og at informasjonssikkerhet ikke bare skal være er et tema for *folka på IT-avdelingen* (Tranvik 2009:23). På lik linje med bestemmelser om internkontroll og regelverk vedrørende helse, miljø og sikkerhet (HMS) er det også her lagt opp til at virksomhetens ledelse har ansvaret. På den måten kan og skal ledelsen sørge for å ha kontroll og orden i eget hus.

### 1.4.3 Om forholdet mellom informasjonssikkerhet og internkontroll

Informasjonssikkerhet nevnes ofte i sammenheng med internkontroll. Reglene om sikring av personopplysninger jf. pol § 13 og reglene om internkontroll jf. pol § 14 er i all hovedsak basert på samme tankegang (Schartum 2005:105). Det kan diskuteres om informasjonssikkerhet får for mye oppmerksomhet i forhold til internkontroll. Årsaken til det kan være at reglene om internkontroll ikke er detaljerte i samme grad som reglene om informasjonssikkerhet i forskriften.[37] Schartum mener at dette faktum ikke må tolkes dit hen at spørsmål om informasjonssikkerhet er viktigere enn for eksempel internkontroll (ibid.). Datatilsynet tydeliggjør også i sin nye veileder for internkontroll og informasjonssikkerhet at

[37] sml. pof kapittel 2 (informasjonssikkerhet) og 3 (internkontroll)

personvern ikke må eller kan begrenses til informasjonssikkerhet alene.[38] De sier videre at man også må kontrollere at de andre kravene som stilles i lov og forskrift blir innfridd. Pol § 14 pålegger den behandlingsansvarlige plikt til å etablere rutiner som fører kontroll med at lovens krav til behandling av personopplysninger blir etterlevd. På lik linje med § 13 krever § 14 at arbeidet skal være forankret hos ledelsen og bygge på planlagte og systematiske tiltak. Hovedforskjellen mellom pol §§ 13 og 14 er at bestemmelsene om internkontroll er gitt for at den enkelte virksomhet skal ha rutiner som sørger for at *alle* rettslige krav blir etterlevd,[39] mens § 13 regulerer sikkerhet spesielt. På den måten kan man si at arbeid med internkontroll hovedsakelig krever juridisk fagkompetanse. Arbeid med informasjonssikkerhet krever en mer teknisk kompetanse, selv om det også her må forutsettes nok juridisk kompetanse til å forstå reglene vedrørende informasjonssikkerhet (Schartum 2005:105). På bakgrunn av dette kan man si at kravene til sikring av personopplysninger utgjør en detaljert del av den komplette internkontrollen. Figuren nedenfor illustrerer forholdet mellom internkontroll og informasjonssikkerhet og viser til at informasjonssikkerhet i denne sammenheng kan forstås som en del av internkontrollen. Jeg går ikke nærmere inn på forholdet mellom internkontroll og informasjonssikkerhet i denne oppgaven.




**Figur 3. Regelverket om sikring av personopplysninger kan ses på som en del av den totale internkontrollen.**

[38] Datatilsynets veileder om internkontroll og informasjonssikkerhet 2009:3
[39] Ved gjennomføring av internkontroll skal man legge særlig vekt på å sikre at kvaliteten på personopplysningene som behandles er god nok jf pol § 14 første ledd. Se for øvrig f. eks Coll & Lenth 2000:110 flg.

### 1.4.4 Om forholdet til annet regelverk

Personopplysningsloven anses som en generell lov. Det er viktig å merke seg at det finnes andre lover og forskrifter som inneholder *spesielle* regler på bestemte områder som for eksempel informasjonssikkerhet (Schartum 2005:100). Dette er fordi noen regler er mer spesialisert og tilpasset mer konkrete tilfeller/områder enn andre (Boe 2004:335).[40] I denne oppgaven vil ikke reguleringer i særlovgivningen bli diskutert inngående, men det er verdt å merke seg at en kan støte på regler av denne karakter.

Problemstillingene som tas opp her er rettet mot kommunal sektor. Forvaltningsloven (heretter: fvl) med tilhørende forskrifter er derfor relevant.[41] Etter fvl § 1 gjelder loven i utgangspunktet *et hvert organ for stat eller kommune*. Særlig interessant i oppgavens sammenheng er fvl § 13 som regulerer taushetsplikt. I første ledd slås det fast at alle som gjør tjeneste eller arbeider for et forvaltningsorgan plikter å unngå at uvedkommende for tilgang til opplysninger om blant annet *noens personlige forhold*.[42] Bruken av betegnelsen noens personlige forhold er ikke i tråd med pol sin terminologi og definisjon av personopplysninger. Det er imidlertid klart at også forvaltningsloven inneholder regler som skal hindre urettmessig spredning av personopplysninger (Schartum 2007:238 flg.). Bestemmelsene om taushetsplikt i fvl kan også koples til konfidensialitetsbegrepet som vi har sett er et sentralt element innenfor informasjonssikkerhet.[43]

eForvaltningsforskriften (heretter: efvf) kan og knyttes til informasjonssikkerhetsarbeid i kommuner.[44] Denne har som formål å legge føringer for sikker og effektiv bruk av elektronisk kommunikasjon i og med forvaltningen jf. § 1, nr. 1. Forskriften henviser også i sin § 13, nr. 3, bokstav g til personopplysningsforskriftens kapittel 2. Forskriftene må derfor ses i sammenheng når det gjelder informasjonssikkerhet og elektronisk kommunikasjon og saksbehandling i og med kommunene.

---

[40] Dette bygger på lex specialis prinsippet som går ut på at spesiell regel går foran generell regel ved regelkollisjon. (For en videre innføring i dette prinsippet, se for eksempel Boe – innføring i jus 2004 side 335 flg.)

[41] Lov 10. feb. 1967 Lov om behandlingsmåten i forvaltningssaker.

[42] Jf. fvl § 13 første ledd nr. 1

[43] Bestemmelsene i pol og fvl er ikke harmoniserte, men dersom en skulle jobbet mot harmonisering kunne det vært nærliggende å anta at pol sin forståelse av personopplysinger – sensitive eller ikke, ville blitt gjeldene. Dette begrunnes i at pol er fundert i personverndirektivet som Norge er forpliktet til etter EØS avtalen (Schartum 2007:241).

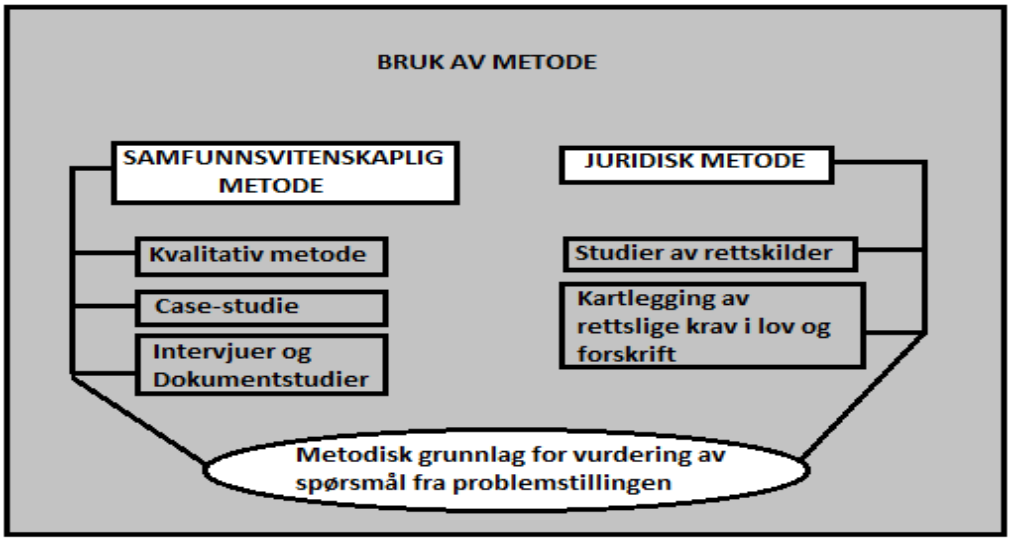
[44] Gitt med hjemmel i fvl. § 15a og lov om elektronisk signatur (esignaturloven) 15. juni 2001 nr. 81.

Det finnes flere lover og tilhørende forskrifter som regulerer informasjonssikkerhet, men jeg har kun nevnt de jeg anser som særlig relevante for denne oppgaven.[45]

[45] For en videre drøftelse av annet relevant lovverk. Se for eksempel Schartum 2005:100 flg.

## 1.5 Om bruk av metoder og kilder

I denne oppgaven har jeg gjennomført et case- studie og har primært benyttet meg av tre typer kilder. Dokumentstudier, intervjuer og rettskilder. Juridiske analyser utgjør en sentral del av det metodiske, men selve undersøkelsen av caset og kartlegging av praksis utredes ved hjelp av dokumentstudier og intervjuer basert på en samfunnsvitenskaplig kvalitativ metode. På bakgrunn av dette kan det metodiske opplegget deles i to, slik figuren under viser:




**Figur 4. Figuren viser hvordan både samfunnsvitenskaplig metode og juridiske analyser må benyttes for å besvare de spørsmål som blir tatt opp i denne oppgaven.**

### 1.5.1 Om bruk av case- studier[46]

Mitt utgangspunkt for å velge case- studie som fremgangsmåte var at jeg ønsket å se på hvordan juridiske og organisatoriske problemstillinger ble løst i praksis. Dette er et omfattende arbeid og krevde en intensiv tilnærming. Jeg anså derfor case- studie som den beste løsningen.

Caset som er valgt kan neppe betegnes som unikt. Likevel er det ikke alt for mange tilfeller av interkommunale IKT- samarbeider. I 2008 ble det antatt å være omkring 35-40 interkommunale IKT-samarbeid i Norge (Lanestedt 2008:19).

| **Organisasjonsform** | **Antall samarbeid** |
|---|---|
| Kml. §27 | 5 |
| Hybrid[47] | 1 |
| IKS- loven | 6 |
| Løst samarbeid | 5 |
| Lov om aksjeselskap | 2 |
| Vertskommune-modellen | 6 |
| Usikkert[48] | 2 |

**Tabell 1 oversikt over ulike organisasjonsformer for interkommunale IKT- samarbeid som er registrert på www.iktsamarbeid.no**

Innenfor dette antallet er det også mye variasjon i valg organisasjonsform, antall medlemmer og hvor omfattende samarbeidet er.[49] Nettstedet www.iktsamarbeid.no har som mål å tilby en oversikt over IKT- samarbeid som finnes i Norge. Ut i fra Lanestedt sine tall kan man anta langt i fra alle IKT- samarbeid har registrert seg i denne databasen. Per dags dato er det kun 27 registrerte samarbeid her.[50] Tabell 1 viser at det blant disse samarbeidene er 5 forekomster av § 27-samarbeid.

### 1.5.2 Om dokumentstudier og intervjuer

Mye av opplysningene som brukes i oppgaven er hentet fra dokumentasjon om og av samarbeidsorganisasjonen. Ved siden av dette har det også vært nødvendig å gjennomføre intervjuer. Dette for å få kommentarer knyttet til dokumentasjonen, for å få supplerende kilder og for å få førstehåndskilder der dokumentasjon ikke finnes eller ikke kan utleveres.

[46] I denne oppgaven har jeg besluttet å se på ett bestemt case eller tilfelle. Dette beskrives i samfunnsvitenskaplig metode som case- studier. Med dette mener man studier der selve studieobjektet (det, de eller dem man studerer) er avgrenset i tid og rom (Jacobsen 2002:71). En ser på et spesifikt miljø eller en spesifikk hendelse. Dette gjør gjerne case- studier til en intensiv og detaljert studie (Grønmo 2007:414).
[47] Jeg har selv valgt betegnelsen hybrid, ut i fra at samarbeidet er organisert i en konstellasjon av ulike hjemler
[48] Fortsatt ikke etablert, men planene er registrert på www.iktsamarbeid.no
[49] IKT- samarbeid består i gjennomsnitt av fem-seks kommuner (Lanestedt 2008:19)
[50] 17.8.2010

#### *1.5.2.1 Dokumentstudier*[51]

Det er særlig fire dokumenter som er sentrale i forbindelse med studien av caset. Disse fikk jeg tildelt ved mitt første møte med samarbeidsorganisasjonen. 1) Før samarbeidet ble inngått ble det utarbeidet en prosjektrapport som omhandlet kommunenes forutsetninger, motiver og ambisjoner ved inngåelsen av samarbeidet. I samme dokument blir det også utredet hva samarbeidet skal jobbe med og hvordan dette påvirker den enkelte kommune. 2) Samarbeidets vedtekter. 3) En Service Leverings Avtale (SLA) som alle kommunene og ledelsen i samarbeidsorganisasjonen har skrevet under på og hvor partenes ansvar og plikter er regulert.[52]4) Samarbeidsorganisasjonens styre har også vedtatt at det skal utarbeides felles retningslinjer for internkontroll og informasjonssikkerhet. Veilederen er utarbeidet av en arbeidsgruppe i samarbeidsorganisasjonen.

I tillegg til disse fire dokumentene ble jeg også tildelt et par multimedie- presentasjoner som ledelsen brukte i foredragsøyemed.

I tillegg til dokumentasjon fra samarbeidsorganisasjonen har jeg benyttet meg av kilder hentet fra ulike aktører innenfor informasjonssikkerhet og interkommunalt samarbeid. Representanter fra Datatilsynet, KS og Direktoratet for forvaltning og IKT. Gjennom disse har jeg fått tilgang til henholdsvis tilsynsrapporter, rapporter som interkommunalt IKT-samarbeid og rapporter vedrørende informasjonssikkerhet.

#### *1.5.2.2 Intervjuer*

Intervjuene som er blitt foretatt i forbindelse med oppgaven kan deles i to. Den første gruppen kan betegnes som fageksperter.[53] I startfasen av arbeidet hadde jeg samtaler med personer på ledelsesnivå i Datatilsynet, KINS samt en representant for KS advokatene for å få deres kommentarer til gjeldende rett og praksis.

---

[51] I samfunnsvitenskaplig metode er dokumentstudier betegnelsen på innhenting, behandling og tolkning data en ikke har utarbeidet selv (Jacobsen 2002:128). Disse kildene kalles sekundærdata fordi sekundærdata i motsetning primærdata ikke er samlet inn av forskeren selv.

[52] Service Leverings Avtale (forkortet som SLA – avtale) er en fornorsking av Service Level Agreemet. I utgangspunktet er hovedfokuset i slike avtaler at IT-servicen fra en leverandør fastslås og at dette avtalefestes. Dette er en kontraktstype som blir mye brukt i IKT- sammenheng. Daler et al. hevder at en gjennom SLA-avtaler også må stille krav til sikkerhet (Daler et. al 2006:208). Han viser også til at det i slike avtaler er særlig viktig at ansvar og eventuelle konsekvenser av kontrakts- mislighold blir definert (ibid. 2006:257). Vi kan her trekke en parallell til sikkerhetskravene i pol og pof som krever klare ansvars og myndighetsforhold.

[53]I samfunnsvitenskaplig metode betegnes disse som informanter. En informant er en person som ikke selv har opplevd det en skal undersøke (som i dette tilfellet betyr at han/hun ikke er en del av caset), men som har god kunnskap om det fagfeltet som studeres (Jacobsen 2002:156).

Den andre gruppen som ble intervjuet var personer med tilknyting til caset.[54] Ved utvelgelse av hvem jeg skulle intervjue valgte jeg å legge vekt på å få samtaler med personer på ledelsesnivå både i samarbeidsorganisasjonen og i deltakerkommunene. Dette begrunnes ut i fra at organiseringen av informasjonssikkerhetsarbeid skal være forankret hos ledelsen og at det er på dette nivået beslutningsmyndigheten ligger. Det var også nødvendig å snakke med personer noe lengre ned i hierarkiet. Dette fordi delegasjonsadgangen er hyppig brukt og undersøkelser viser at toppledelsen på kommunalt nivå ikke alltid har inngående kunnskap og fokus rundt informasjonssikkerhet.[55] Dermed har det vært nødvendig å prate med noen som er involvert i det praktiske arbeidet. De jeg har snakket med sitter enten med et formelt ansvar, operasjonelt ansvar eller teknisk ansvar/kompetanse i forhold til informasjonssikkerhetsarbeidet. I prosessen med å finne intervjuobjekter fikk jeg assistanse av en rådgiver i samarbeidsorganisasjonen. Han pekte meg i retning av virksomhetsledere som han mente kunne gi svar på mine spørsmål på vegne av deltakerkommunene. Selv kontaktet jeg rådmenn pr. telefon eller e-post for å avtale intervjuer.

Intervjuformen jeg har brukt betegnes i samfunnsvitenskaplig metode som semistrukturerte intervjuer. Totalt ble det foretatt 10 informant- intervjuer. Noen intervjuer ble foretatt ansikt til ansikt. Dette gjelder intervjuene gjort med daglig leder i samarbeidsorganisasjonen, rådgiver fra samarbeidsorganisasjonen, rådmennene i kommune 2 og 3 og en virksomhetsleder i kommune 1. Resten av intervjuene ble foretatt over telefon, dette på grunn av reiseavstander og intervjuobjektenes tidsskjema. Ved flere anledninger har det vært behov for å avklare detaljer. Dette har blitt løst enten gjennom oppfølgingsintervjuer over telefoner eller korrespondanse over e-post.[56] Flere av intervjuene ble tatt opp med diktafon. Ved intervjuer gjennomført over telefon benyttet jeg ikke diktafon. Intervjuene varte i gjennomsnitt mellom 30 til 45 minutter.

Gjennomføring av intervjuene gikk stort sett bra, men når det kom til kommune 1 møtte jeg noen utfordringer. Ved forsøk på å snakke med noen representanter fra kommune 1 ble jeg direkte henvist til samarbeidsorganisasjonen. Dette var et problem fordi jeg dermed ikke ville få innblikk i hvordan kommunen selv organiserte sitt arbeid med informasjonssikkerhet. De mente på sin side at informasjonssikkerhet var IKT og at spørsmål om IKT ble løst av

[54] I samfunnsvitenskaplig metode kaller vi denne typen intervjuobjekter for respondenter. Noen som selv har opplevd det vi ønsker å studere (Jacobsen 2002:156)
[55] Se bl.a. Tranvik 2009:51 og Datatilsynets årsmelding 2003:24 flg.
[56] Det var særlig intervjuer foretatt over telefon og uten diktafon at oppfølgingssamtaler ble nødvendig.

samarbeidsorganisasjonen. Jeg vurderte å be om innsyn etter personopplysningslovens § 18 for å få de mest nødvendige opplysningene om kommunens behandling av personopplysninger, samtidig som jeg henvendte meg til Datatilsynet for å se om de hadde noen kontrollrapporter som kunne belyse organiseringen av informasjonssikkerhetsarbeid i kommunen. Parallelt med å forfatte en innsynsbegjæring hadde jeg kontakt med en rådgiver i samarbeidsorganisasjonen, som nevnte to personer i kommunen jeg kunne forsøke å snakke med. Først fikk jeg kun kontakt med en av dem, en virksomhetsleder/systemeier, dermed ble det ikke nødvendig å be om innsyn. Kommunen hadde hatt Datatilsynet på besøk og jeg besluttet å be om kopier av rapporten som supplerende materiell. Helt på tampen av arbeidet med oppgaven fikk jeg også kontakt med en rådgiver i kommunen som jeg også hadde henvendt meg til. Jeg tror ikke at disse utfordringene har påvirket resultatet på oppgaven i annet henseende enn at det har tatt litt ekstra tid og at respondentenes svar på mine spørsmål har blitt spredt litt mer i oppgaveteksten enn jeg opprinnelig hadde ønsket. De problemene jeg hadde kan også tolkes som et tegn på at man i denne kommunen fortsatt tenker at informasjonssikkerhetsspørsmål er kun noe IKT avdelingen driver med (se for øvrig kapittel 3).

Ved starten av arbeidet med oppgaven hadde jeg ikke gjort meg noen tanker om hvorvidt samarbeidsorganisasjonens navn, kommunenes navn og respondentenes navn skulle nevnes eller ikke. Jeg bestemte meg for dette først etter en av mine første intervjuer. Intervjuobjektet sa at det var greit at jeg brukte diktafon dersom ikke navn ble nevnt i oppgaven. Ut i fra dette vurderte jeg det slik at anonymitet ville bidra til en mer ærlig og åpen dialog med respondentene. I intervjuene som ble foretatt etter dette opplyste jeg respondentene om at ingen navn kom til å bli brukt i oppgaven. Samtidig har ikke oppgaven til hensikt å avsløre eller rapportere om informasjonssikkerhetsarbeidet i kommunene eller det interkommunale IKT- samarbeidet. I det henseende er det uten betydning hva kommunene og menneskene som jobber der heter. Representantene fra samarbeidsorganisasjonen hadde tilsynelatende ingen problemer med at jeg anga navn på samarbeidet i oppgaven og jeg har heller ikke skrevet under på noen taushetserklæring. I forbindelse med at jeg skulle anonymisere respondentene valgte jeg likevel å anonymisere hele caset. Dette begrunner jeg med anonymisering av selve caset styrker intervjuobjektenes/respondentenes grad av anonymitet ytterligere.[57]

[57] Ulempen med anonymitet knyttet til respondenter og case er at en kan reise spørsmål om mulighetene for å etterprøve de data som blir presentert i oppgaven. Ved å være tydelig på bruk av metode og undersøkelsesdesign

### 1.5.3 Om juridisk metode knyttet til de rettsdogmatiske analysene

Problemstillingen i denne oppgaven har i stor grad en juridisk vinkling med særlig fokus på rettsområdet informasjonssikkerhet i forhold til behandling av personopplysninger. En god del av arbeidet er derfor basert på analyse av ulike rettskildefaktorer. Problemstillingen krever oversikt over gjeldende rett på området, blant annet fordi den innebærer vurderinger av praksis innen et interkommunalt IKT- samarbeid. I problemstillingen tar jeg utgangspunkt i lov om behandling av personopplysninger[58] og den tilhørende forskriftens kapittel 2.[59] Det er disse lov- og forskriftstekstene som danner utgangspunktet for min utlegning av gjeldende rett.

Lov- og forskriftstekster er ofte helt sentrale rettskildefaktorer.[60] Også andre rettskilder vil imidlertid være nødvendige for å kartlegge rettstilstanden på tilstrekkelig måte.

Lovforarbeider er en sentral rettskildefaktor i denne oppgaven. Det er særlig Ot. prp nr 92 (1998-99) og innstillingen fra stortingets fagkomité, innst. O. nr 51 (1999-2000) som blir benyttet. Forarbeidene, særlig proposisjonen, er en viktig kilde fordi de på flere punkter utdyper og presiserer lovteksten. Samtidig gir forarbeidene et større innblikk i tankegodset som ligger bak lovteksten og kan således gi uttrykk for hensynet bak bestemmelsene. En kan argumentere for at forarbeidene ikke kommenterer informasjonssikkerhet konkret og derfor at de ikke kan tillegges for mye vekt.[61] På en annen side er det mange diskusjoner og begreper knyttet til pol som forarbeidene tar nøye for seg. Disse er igjen viktige i forhold til problemstillingen. Dette gjelder særlig avklaringer vedrørende definering av roller og ansvar innunder aktørene behandlingsansvarlig og databehandler (se for øvrig oppgavens kapittel 2).

Jeg vil også trekke frem Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 – *om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger*. Norge er gjennom EØS avtalen pålagt å vedta lovgivning som er i samsvar med direktivet (Boe 98:2004). Forarbeidene til pol gir uttrykk for at de ønsker en norsk lov som er i tråd med direktivet. På denne måten kan man bruke direktivet

---

kan en bøte litt på dette punktet, fordi man gjennom dette viser oppskriften man har bukt. Dermed også hvordan en har kommet fram til de konkrete resultatene som blir presentert. (se for øvrig Fossheim 2009. http://etikkom.no/no/FBIB/Temaer/Personvern-og-ansvar-for-den-enkelte/Konfidensialitet/)

[58] Lov av 14. april 2000 nr.31

[59] Forskrift av 15. desember 2000 nr 1265

[60] For mer om lovtekst som rettskildefaktor. Se for eksempel Boe 2005: 137

[61] Dette fordi bestemmelsen om informasjonssikkerhet i pol er svært generell og en må gå til forskriftens kapittel 2 for utdypende bestemmelser.

som sammenligningsgrunnlag eller referanse der personopplysningsloven kan virke uklar. Det antas ellers at personopplysningsloven og direktivet er i samsvar.

*Rettspraksis* gjør seg ikke i nevneverdig grad gjeldende i denne oppgaven. Jeg foretok søk i domsregisteret på Lovdata på søkeordene *personvern* og *informasjonssikkerhet*.[62] Det finnes mange høyesterettsdommer som på ulike måter berører personvern. Det lyktes meg likevel ikke å finne dommer fra noen av instansene som kan sies å være direkte relevante.[63]

*Forvaltningspraksis* fra Datatilsynet er benyttet i denne oppgaven. Jeg tillegger Datatilsynets generelle praksis og anbefalinger i form av skriv, maler og veiledere en del vekt i drøftelsen når lov eller forskrift ikke er helt klar. Et eksempel her kan være at forskriftens § 2-4 annet ledd krever at den behandlingsansvarlige skal gjennomføre risikovurderinger. Bestemmelsen sier imidlertid ikke mye om hvordan dette skal gjennomføres i praksis. Her og ved andre anledninger har Datatilsynets veiledningsmateriell bidratt til å gi større klarhet i hvordan lov og forskrift kan implementeres i praksis. Jeg har også sett på noen tilsynsrapporter fra Datatilsynet. Disse tillegges normalt vekt dersom de ikke har blitt omgjort etter klage til Personvernnemnda.

Personvernnemnda er klageorganet for Datatilsynet og nemndas praksis bør tillegges relativt stor vekt. Jeg foretok søk på Personvernnemndas nettsider[64] og fant noe relevant materiell[65]. Ved motstrid vil Personvernnemndas praksis normalt ha større vekt enn Datatilsynets praksis.

En siste rettskildefaktor som er tatt med og vektlagt i denne oppgaven er *juridisk teori*. I klassisk rettskildelære anses dette å være en faktor som ligger under de andre rettskildefaktorene i hierarkiet. Hvordan man anvender og vekter denne rettskildefaktoren avhenger av hvem som står bak og i hvilket øyemed innholdet er utformet**.** Dersom en gjør bruk av juridisk teori er det viktig å sammenligne alternative kilder. På den måten kan man finne frem til uenigheter og få et bredere perspektiv på rettsspørsmålene. I denne oppgaven

[62] www.lovdata.no
[63] Det foreligger et par dommer hvor spørsmål om avskjedigelse for brudd på interne sikkerhetsbestemmelser diskuteres, se: HR-2005-00649-A og Dom: 2004-03-03. LB-2003-9695.
[64] http://www.personvernnemnda.no/
[65] Jeg benyttet søkeordene ”informasjonssikkerhet” og ”kommune”. Av interesse her var PVN-2006-07 og PVN-2007-04 Den første omhandler Tysvær kommunes bruk av biometri (avlesning av brukeres fingeravtrykk) for å logge inn på datamaskiner eid av kommunen. Kommunen anførte i utgangspunktet at tiltaket var begrunnet i informasjonssikkerhet. Selve vedtaket og klagen er i hovedsak en diskusjon om rettslig grunnlag og pol § 12 (om entydige identifikatorer). Den andre saken er av større interesse. Dette er en klage fremsatt av Rogaland fylkeskommune. Vurderingene gjort av nemnda omhandler kort sagt hva som skal anses som en tilfredsstillende risikovurdering og drøfting av Datatilsynets veiledningsplikt. Risikovurderinger blir behandlet i oppgavens kapittel 3.

har jeg tillagt teori vekt ved flere anledninger. Referansene er særlig hentet fra professor Dag Wiese Schartum og førsteamanuensis Lee A. Bygrave på juridisk fakultet ved Universitetet i Oslo. Begge blir ansett som eksperter på feltet og den delen av deres litteratur jeg benytter meg av er av *de lege lata* karakter. Det vil si at tekstene anses å være drøftelser og vurderinger av gjeldende rett m.m. Jeg benytter meg også av personopplysningslovens kommentarutgave som kan sies å ligge i grenseland mellom rettsanvenders praksis og juridisk teori. Denne boken er skrevet av Michal Wiik Johansen m.fl. Alle forfatterne har fartstid i Datatilsynet, og en av forfatterne har vært med på utarbeidelsen av personopplysningsforskriften. Boken byr på en systematisk gjennomgang av bestemmelsene i lov og forskrifter med tilknyttede kommentarer. *Personopplysningsloven – en håndbok* skrevet av Line Coll og Claude A. Lenth har også blitt brukt som en alternativ kilde. Denne boken ble gitt ut før forskriften ble vedtatt. Dette faktum preger litt av diskusjonen om informasjonssikkerhet i boken. Til tross for dette inneholder boken mange gode redegjørelser og diskusjoner om personvern som er relevant for problemstillingen. Jeg benytter meg av denne referansen særlig ved diskusjon om forholdet mellom internkontroll og informasjonssikkerhet og diskusjoner knyttet til behandleransvar og databehandlere.

## 1.6 Noen ord om tidligere forskning

Det er gjort forskning som på flere måter er relevant for problemstillingen i denne oppgaven. Jeg begynte å lete etter kilder i det forvaltningsinformatiske miljøet. Her visste jeg det var gjort lignende forskning tidligere. Gjennom disse kildene fant jeg referanser til annen relevant litteratur. Jeg benyttet meg også av kildesøk i Bibsys. Det finnes svært mye litteratur om kommuner og informasjonssikkerhet hver for seg. Det var først når jeg sammenholdt disse søkeordene at jeg fikk bedre oversikt over aktuelle kilder.

Ved siden av søk på internett har jeg også fått anbefalt rapporter av personer med kjennskap til miljø omkring informasjonssikkerhet og interkommunale samarbeid. Jeg nevner særlig "Interkommunalt samarbeid i Norge – omfang og politisk styring" som er en rapport utarbeidet ECON på oppdrag for KS.[66]

I forhold til relevant forskning på informasjonssikkerhetsfeltet vil jeg trekke frem to rapporter knyttet informasjonssikkerhet i offentlig sektor. "Utredning av behov for sertifisering av sikkerhetskompetanse blant IKT- personell i offentlig sektor" som er utarbeidet av Security Valley på oppdrag fra Fornyings og administrasjonsdepartementet (FAD) og ble ferdigstilt i mars 2009. Rapporten er basert på spørreundersøkelser som ble sendt ut til kommuner, fylkeskommuner og statlige etater. Rapporten konkluderer blant annet med at det er behov for kompetanseheving hos IKT- ansatte.

En annen rapport jeg vil karakterisere som relevant er "Security Awareness Management in local Governments: Approaches in Scandinavia".[67] Denne rapporten er fra oktober 2008 og er utarbeidet av European Network and Information Security Agency (ENISA). Rapporten er basert på en spørreundersøkelse sendt ut til kommuner og fylker i Norge, Sverige og Danmark og resultatet viser blant annet at mange kommuner mangler elementær dokumentasjon vedrørende informasjonssikkerhet og at så mange som 25 % av de spurte mangler dokumenterte retningslinjer, samt at roller og oppgaver er uklare. Bare under halvparten av respondentene har en sikkerhetsansvarlig i full stilling.

[66] Econ analyse, rapport 2006 -057.
[67] Den komplette undersøkelsen er tilgjengelig på:
http://www.enisa.europa.eu/act/ar/deliverables/2008/scandinavian-approaches-survey

Til tross for den forskningen jeg har henvist til over er det likevel i det "forvaltningsinformatiske miljøet" jeg har funnet mest relevant informasjon.

Tommy Tranvik har gitt ut flere publikasjoner der informasjonssikkerhetsarbeid i Norske kommuner er i fokus. Mest relevant for denne oppgaven er nok "Personvern og informasjonssikkerhet – en studie av rettsreglers etterlevelse i kommunal sektor" (Tranvik 2009). Her har han ved omfattende analyse av 19 kommuners organisering av informasjonssikkerhetsarbeid kommet frem til at det gjennom en *etterlevelsesillusjon* gis inntrykk av at kommuner ivaretar regelverket i større grad enn det de faktisk gjør, uten at dette bygger på kalkulert kynisme fra kommunenes side. Det er heller snakk om at brist i flere organisatoriske forhold skaper denne illusjonen. Med organisatoriske forhold menes for eksempel manglende forankring hos ledelsen, liten involvering av øvrige ansatte og mer eller mindre sporadisk arbeid med rutiner og dokumentasjon. Tranvik sitt arbeid er relevant fordi det nettopp drøfter hvordan kommuner løser utfordringer knyttet til organisering av informasjonssikkerhetsarbeid. Likevel blir ikke dette i nevneverdig grad behandlet i lys av interkommunale IKT- samarbeid.

Are Vegard Haug har forsket mye på IKT og kommuner. Det er særlig to av hans publikasjoner jeg benytter meg av. Den første er "Rettslige reguleringer av informasjonssikkerhet" fra 2006 (Haug 2006). Her har han sett på hvordan norske myndigheter regulerer informasjonssikkerhet gjennom lover og forskrifter. Særlig interessant for denne oppgaven er hans beskrivelse av informasjonssikkerhet i forhold til personopplysningsvern. Den andre er Haug sin doktoravhandling fra 2009 "Lokaldemokratiet på nett og i nett" (Haug 2009). Avhandlingens kapittel 4 om organiseringen av IKT- baserte nettverk i norske kommuner er mest interessant her. Haug benytter betegnelsen *kommunale IKT nettverk* og favner i så måte alle samarbeidsordningene uavhengig av samarbeidenes formelle, juridiske og/eller organisatoriske struktur. Hovedfokuset hans er å si noe om hvem som samarbeider om hva og hvorfor. Av interesse for denne oppgaven er også hans tanker om hvorfor kommuner samarbeider om IKT. Kort gjengitt virker årsakene å være at kommunene, uavhengig av størrelse, beliggenhet og demografi, møter økte krav til digitalisering. Dette stiller store krav til økonomisk kapasitet og kompetanse. Haug argumenterer videre for at inngåelse av *grensekryssende IKT- nettverk* fremstår som en rasjonell løsning på kommuners

opplevde IKT- utfordringer og at den eksisterende kommuneoppdelingen i dette henseende er uhensiktsmessig (Haug 2009:122).

Ørnulf Storm skrev sin masteroppgave ved Avdeling for forvaltningsinformatikk i 2009 (Storm 2009). [68] Denne tar også for seg hvordan arbeidet med informasjonssikkerhet organiseres i kommuner. I en av sine konklusjoner argumenterer han for at kommuners engasjement i interkommunale IKT- samarbeid kan gi gevinster til den enkelte kommune med tanke på organisering av informasjonssikkerhetsarbeidet.

Jeg har ikke funnet inngående studier av arbeid med sikring av personopplysninger i interkommunale IKT- samarbeid, men de ovennevnte forskningsarbeidene er alle gode referanser med hensyn til temaene som tas opp i denne oppgaven.

[68] Oppgaven i sin helhet er bl.a. tilgjengelig på: http://www.duo.uio.no/sok/search.html?ORGID=267

## 1.7 Oversikt over den videre fremstillingen

I ***kapittel to*** vil jeg konsentrere meg om partene som inngår i samarbeidet. Det er klart at oppgaver relatert til sikring av personopplysninger er delt mellom den enkelte kommune og samarbeidsorganisasjonen. Det sentrale elementet i dette kapittelet blir derfor å se på hvem som har hvilken myndighet og hvilket ansvar. Det som er interessant her er blant annet å se på aktørene behandlingsansvarlig og databehandler, og hvordan rolle-, ansvars- og arbeidsdelingen er mellom disse. Kapittelet er disponert slik at jeg først presenterer gjeldende rett og problemstillinger av rettslig karakter før jeg anvender disse utgangpunktene på forholdene i deltakerkommunene og i samarbeidsorganisasjonen. Dette gjøres for å kartlegge de formelle kravene lovverket stiller til kommunene og samarbeidet i forhold til sikring av personopplysninger.

I ***kapittel tre*** ser jeg på hvilke oppgaver de enkelte aktørene som ble presentert i kapittel 2 har vedrørende organiseringen av informasjonssikkerhetsarbeidet. Dette kapittelet vil også gi en pekepinn på om de formelle kravene som jeg har redegjort for i foregående kapittel samsvarer med praksis i kommunene og samarbeidsorganisasjonen. I casestudiet inngår tre relativt små kommuner og her viser det seg at noen personer har mer enn en rolle knyttet til sikkerhetsarbeidet. Jeg kommer også til å se på hvorvidt den opprettede samarbeidsorganisasjonen har tatt på seg noen av oppgavene som i utgangspunktet har ligget til den behandlingsansvarliges virksomhet. Vi skal senere i kapittelet se at dette er tilfellet og det kan diskuteres om dette er hensiktsmessig eller om det svekker den enkelte behandlingsansvarliges kontroll over organiseringen av sikkerhetsarbeidet.

I ***kapittel 4*** vier jeg oppmerksomheten til drøfting av hvorvidt og i hvilken grad det interkommunale IKT- samarbeidet påvirker deltakerkommunenes arbeid med informasjonssikkerhet. Gjennom kapitlene 2 og 3 ser vi hvordan roller, ansvar og oppgaver er fordelt og hvilken rolle samarbeidsorganisasjonen spiller. Drøftelsene som gjøres i dette kapittelet vil bygge på konklusjonene av de to foregående kapitlene. Her oppstår en interessant diskusjon om hvorvidt typiske kvaliteter ved samarbeid, som for eksempel kompetanseheving og økte ressurser bidrar til bedre oppgaveløsning, her sett i lys av organisatoriske forhold omkring arbeidet med sikring av personopplysninger. Også spørsmålet om det er samsvar mellom de formelle kravene (kapittel 2) og det praktiske arbeidet (kapittel 3) blir viet oppmerksomhet. Dersom det viser seg å ikke være samsvar mellom det formelle og det praktiske, blir spørsmålet hvilke konsekvenser dette får for

kommunenes arbeid med informasjonssikkerhet, og om vi kan trekke noen praktiske lærdommer fra måten informasjonssikkerhetsarbeidet er organisert i deltakerkommunene og samarbeidsorganisasjonen?

I ***kapittel 5*** oppsummeres arbeidet og de funnene som er gjort. Jeg stiller også noen spørsmål om eventuelle løsninger på de utfordringer som har blitt presentert og noe om veien videre.

## 2 Avklaring av ansvar og myndighet

I avsnitt 1.1 nevnte jeg at en viktig faktor for at et samarbeid om informasjonssikkerhet skal lykkes er at forhold som gjelder ansvar, myndighet og fordeling av oppgaver er avklart. Dette har også blitt understreket av Datatilsynet. Kommunene og samarbeidet har i fellesskap utarbeidet dokumentasjon og avtaleverk som regulerer disse forholdene.

Fra problemstillingen:

1. Hvordan er de rettslige ansvars- og myndighetsforholdene fordelt mellom deltakerkommunene og organet for det interkommunale IKT- samarbeidet?

    a. I hvilken grad er disse forholdene dokumentert?
    b. I hvilken grad er disse forholdene i samsvar med lov og forskrift?

## 2.1 Aktørene

Et sentralt moment for å forstå og overholde regelverket er at den enkelte kommune og det interkommunale IKT- samarbeidet har klare rammer for hvem som gjør hva (Schartum & Bygrave 2006:34). I redegjørelsen bruker jeg begrepene *aktører* og *roller* (se avsnitt 2.4 flg.). Jeg skiller mellom betegnelsene aktører og roller i den forstand at en aktør er en fysisk eller *juridisk person*[69] mens en rolle angir ulike funksjoner som ligger under den enkelte aktør. Ved behandling av personopplysninger er det alltid to aktører. Den registrerte[70] og den behandlingsansvarlige. Ofte oppstår det en aktør til, databehandleren. Dette blir aktuelt dersom behandlingsansvarlig gjør seg til oppdragsgiver og får en annen virksomhet til å behandle personopplysninger på sine vegne. I avtaleverket mellom deltakerkommunene og IKT- samarbeidet blir aktøren databehandler aktualisert. I SLA – avtalen og i den felles veilederen for internkontroll og informasjonssikkerhet blir deltakerkommunenes rådmenn utpekt som behandlingsansvarlige og IKT- samarbeidet blir betegnet som databehandler. Jeg skal i det følgende gå igjennom lovens regulering av disse to aktørene og se hvordan kommunenes og samarbeidets forståelse av disse begrepene er forenelig med lovens bokstav. Deretter vil jeg se nærmere på hvordan roller er organisert innenfor den enkelte aktørs virksomhet.

[69] En juridisk person er en betegnelse på et rettssubjekt som ikke er en fysisk person eks. selskaper, offentlige og private organisasjoner, foreninger etc. (Boe 20:2005)
[70] Den eller de som personopplysningene omhandler jf. pol § 2 nr 6

## 2.2 Behandlingsansvaret

Den behandlingsansvarlige betegnes som personopplysningslovens "hovedaktør" (Schartum & Bygrave 2004:124). Den behandlingsansvarlige har også hovedansvaret når det gjelder organiseringen av arbeidet med sikring av personopplysninger. I pol § 13 er det angitt at den behandlingsansvarlige har ansvaret for tilfredsstillende informasjonssikkerhet. Å fastslå hvem som er behandlingsansvarlig er derfor svært viktig.

### 2.2.1 Rettslige utgangspunkter

Behandlingsansvarlig ble innledningsvis (avsnitt.1.4.2) nevnt som den som bestemmer formålet med behandlingen av personopplysningene og de hjelpemidler som skal tas i bruk jf. pol § 2, nr. 4. Lovens definisjon bygger på definisjonen som finnes i personverndirektivets artikkel 2 d:

*[…] Den fysiske eller juridiske person, offentlig myndighet, byrå eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandling av personopplysninger og hvilke hjelpemidler som skal benyttes[…]* [71]

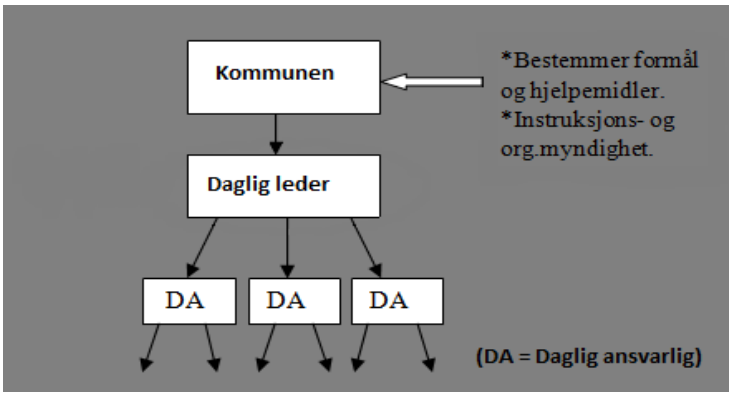
Definisjonen i pol er ikke like utfyllende og skjelner ikke mellom fysiske, juridiske, offentlige eller andre personer og virksomheter. Det er likevel klart at loven gjelder for offentlige så vel som private virksomheter og personer.

For å fastslå hvem som er behandlingsansvarlig er det naturlig å starte med definisjonen i pol § 2 nr. 4. Lovteksten angir at det er den som bestemmer *formålet* med behandlingen og videre hvilke *hjelpemidler* som skal brukes som er behandlingsansvarlig. Som et utgangspunkt kan en derfor anta at det organet eller den personen med slik myndighet blir å anse som behandlingsansvarlig. I denne oppgaven er det virksomheter, nærmere bestemt forvaltningsorganer som blir vurdert. Jeg går derfor ikke videre inn på enkeltpersoner som behandlingsansvarlige.

Loven gir ikke alltid klart svar når det gjelder hvem som er eller kan være behandlingsansvarlig og dermed kan det være behov for presiserende avgrensninger. Videre vil jeg derfor ta opp problemstillinger vedrørende etablering av behandlingsansvar som er særlig relevant for kommuner og interkommunale samarbeid. For andre type virksomheter kan resonnementene være annerledes.

[71] Direktiv 95/46/EU – norskspråklig versjon

Et veiledende moment når en skal fastslå hvem som kan være behandlingsansvarlig er at den behandlingsansvarlige bør ha sivilprosessuell partsevne. Med dette menes det at det fortrinnsvis bør være subjekter med mulighet til å opptre som saksøkt i en tvist for domstolene som er behandlingsansvarlig. Dette er ikke direkte regulert i loven, men av forarbeidene og lovens kommentarutgave (se Johansen et al. 2001:72) må man forstå dette som tilrådelig. [72] Dette begrunnes i muligheten for at noen gjennom rettsapparatet vil kunne sette krav til den behandlingsansvarlige (rettslig ansvarliggjøring).



Figur 5. Kommunens øverste ledelse er behandlingsansvarlig, men kan delegere kompetanse til underliggende nivå

Forarbeidene sier videre at dersom virksomheten er å regne som en juridisk person – som er tilfellet for alle norske kommuner, vil den behandlingsansvarlige være virksomheten, representert ved dennes ledelse.[73] Coll og Lenth skriver at innenfor offentlig sektor vil det være det enkelte forvaltningsorgan eller etat som er behandlingsansvarlig (Coll & Lenth 2000:33). I tilfellet med forvaltningsorgan er det derfor ikke snakk om at én enkelt person er behandlingsansvarlig. En annen diskusjon er hvorvidt ansvaret for at loven etterleves i praksis er tillagt en eller flere bestemte personer.

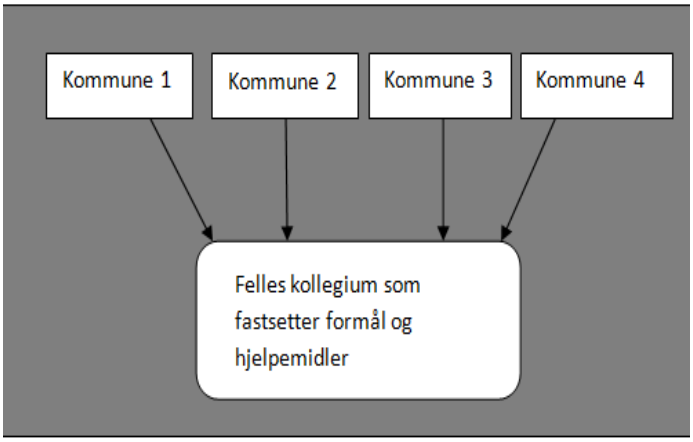
Behandlingsansvaret legges til ledelsen og det er denne som bestemmer formålet og hjelpemidlene. Derav følger det implisitt at den behandlingsansvarlige innehar øverste instruksjons- og organisasjonsmyndighet. Ledelsens oppgave blir deretter å foreta en intern ansvars- og arbeidsfordeling slik at det er klart til hvilken stilling(er) det ligger å ivareta loven til daglig. Pol og pof inneholder ingen bestemmelser som hindrer delegasjon, tvert i mot betegner forarbeidene bruk av delegasjon nærmest som en forutsetning for at lovens krav skal innfris.[74] Ved bruk av delegasjon må en være klar over at man kan delegere kompetanse men ikke ansvar. Dette gjelder også i forhold til behandlingsansvaret:

[72] Ot. prp. nr 92 (1998-99)s.103
[73] Ot. prp. nr 92 (1998-99) s. 102
[74] Ot. prp. nr 92 (1998-99) s. 102

*Den behandlingsansvarlige kan imidlertid ikke fraskrive seg sitt "rettslige" behandlingsansvar ved delegeringen. Det er bare kompetansen som delegeres, ikke ansvaret.*[75]

Det er også viktig å være klar over at selv om den behandlingsansvarlige skulle sette ut selve behandlingen av personopplysninger til andre, vil de fortsatt beholde behandleransvaret med de plikter og ansvar det medfører.[76]

En siste problemstilling som dukker opp ved avklaring av behandleransvaret - og som kanskje er spesielt aktuelt for interkommunale samarbeid, er spørsmålet om *delt behandleransvar*. Schartum og Bygrave skriver at pol åpner for delt behandleransvar og skiller mellom variantene *vertikalt* - og *horisontalt delt* behandlingsansvar (Schartum og Bygrave 2006:30 flg.). Delt behandlingsansvar kommer ikke direkte frem av pol, men direktivet åpner for dette ved å definere den behandlingsansvarlige som den som "alene eller *sammen med andre*" fastsetter formål og hjelpemidler jf. direktivets art. 2 d. Det er kun den vertikale/ hierarkiske varianten som omtales i forarbeidene. Forarbeidene gir i den forbindelse et eksempel fra offentlig sektor der de viser til at et departement fastsetter overordnede formål, mens underliggende direktorat fastsetter hjelpemidlene. På denne måten kan begge organene være behandlingsansvarlig etter loven. [77] Jeg behandler ikke det vertikalt delte behandlingsansvaret videre her, men nevner at Schartum og Bygrave betegner denne type delt behandlingsansvar som uheldig og uhensiktsmessig (Schartum & Bygrave 2006:31).[78]



Figur 6 horisontalt delt behandleransvar

Schartum og Bygrave omtaler horisontalt delt behandlingsansvar som mer aktuelt. Et

[75] Coll og Lenth 2000:37
[76] Ot. prp. nr. 92 (1998-99) s. 103
[77] Ibid.
[78] Dersom det er snakk om et overordningsforhold der for eksempel et departement har kompetanse til å fastsette formål og hjelpemidler vedrørende den behandling som skjer i underordnet direktorat bør behandlingsansvaret i følge Schartum og Bygrave alltid legges til det overordnede organ. Dette vil være uproblematisk fordi den behandlingsansvarliges kompetanse kan delegeres til det underordnede organet som følge av departementets organisasjons- og instruksjonsmyndighet. På den måten vil det overordnede ansvaret være plassert på ett sted samtidig som det daglige arbeidet gjennom delegasjon blir flyttet til det nivået med de beste forutsetningene for å utøve dette. Det vil derfor ikke i disse tilfeller være nødvendig med delt behandleransvar, så lenge instruksjons- og delegasjonsadgangen er til stede.

slikt scenario kan gjøre seg gjeldene der det ikke foreligger noen form for over- eller underordningsforhold (ibid: 32). Et nærliggende eksempel er nettopp interkommunale samarbeid. I og med

at hver enkelt kommune er selvstendig foreligger det ikke noe over – eller underordningsforhold kommunene i mellom. Det er ikke uvanlig at kommuner samarbeider om IKT og i den sammenheng har et eller flere felles informasjonssystemer som behandler personopplysninger. I en slik situasjon kan man tenke seg at kommunene bestemmer formål og hjelpemidler sammen.

Det er likevel viktig at man ikke blander horisontalt delt behandlingsansvar med felles bruk av databehandler (se avsnitt 2.3 om databehandler).

Det kan tenkes at kommuner for eksempel går sammen om felles innkjøpsavtale med en leverandør og at denne leverandøren behandler personopplysninger på kommunenes vegne. En slik ordning vil ikke påvirke den enkelte kommunes bestemmelsesrett over formål og hjelpemidler. Horisontalt delt behandlingsansvar gjør seg altså bare gjeldende når flere aktører som i utgangspunktet har selvstendig behandlingsansvar forplikter seg til å utøve denne bestemmelsesretten i fellesskap.

### 2.2.2 Behandlingsansvar hos kommunene i caset

En kommune regnes som en juridisk person. Etter forarbeidene og kommentarene må vi derfor forstå det slik at det er kommunen, ved dennes ledelse, som er behandlingsansvarlig. I utgangspunktet kan en tenke seg en *ved kommunens ledelse* sikter til ordføreren og hans/hennes apparat. Dette fordi han/hun er kommunens rettslige representant jf. kommuneloven § 9 nr. 3. Denne slutningen er imidlertid ikke forenlig med det deltakerkommunene i caset har bestemt. Fra fremstillingen av behandlingsansvarlig i avsnitt 2.2 så vi at utgangspunktet for å avgjøre hvem som er behandlingsansvarlig er å fastslå hvem som bestemmer formålet med behandlingen og de hjelpemidlene som skal brukes.

Kommunene i samarbeidet har alle definert IKT som en administrativ oppgave og har lagt det overordnede og formelle ansvaret for kommunenes IKT – funksjon til sine respektive rådmenn.[79] Dette fremkommer av avtaleverket mellom partene og ble bekreftet i et intervju

[79] Administrasjonssjefen, populært kalt rådmannen, er kommunens øverste administrative leder jf. § 23 nr. 1 og er en lovpålagt stilling. Administrasjonens hovedoppgaver består i saksforberedende arbeid og iverksetting av politiske vedtak. Når det kommer til kommunenes kjerneoppgaver ovenfor borgere er disse som oftest

med samarbeidsorganisasjonen og representanter fra deltakerkommunene. I forlengelsen av dette blir det naturlig at det er kommunene ved deres rådmenn som er behandlingsansvarlig. Det er neppe spesielt at kommuner tildeler sin rådmann denne oppgaven i stedet for ordføreren når oppgaver relatert til IKT blir definert som et administrativt anliggende og ikke politisk. På den annen side er det etter loven ikke noe i veien for at ordføreren kan være behandlingsansvarlig på kommunens vegne.[80] Datatilsynets årsmelding fra 2003 viser også til at det vanligvis er rådmannsfunksjonen som ivaretar behandlingsansvaret i kommuner.[81]

I prosjektrapporten, SLA - avtalen og i den felles veilederen for internkontroll og informasjonssikkerhet heter det at "Rådmennene i den enkelte kommune er behandlingsansvarlig etter personopplysningsloven." Det å betegne rådmannen som behandlingsansvarlig vil i utgangspunktet ikke være helt treffende. I avsnitt 2.2.1 så vi at det i offentlig sektor vil være forvaltningsorganet ved ledelsen som er behandlingsansvarlig. Når det i dette tilfellet er snakk om behandlinger av administrativ art vil det være kommunen ved rådmannen som er behandlingsansvarlig. Altså ikke rådmannen selv. Rådmennenes rolle blir videre behandlet i avsnitt 2.5.

Hvilket ansvar og hvilke oppgaver som skal utøves av den enkelte person innenfor kommunen som behandlingsansvarlig må - som vi har sett, bestemmes ut i fra en intern arbeidsfordeling. Når kommunene ved deres rådmenn er behandlingsansvarlig, ligger kompetansen til å foreta denne arbeidsdelingen i praksis hos den enkelte rådmannen. Det vil altså være han/hun som utøver den øverste instruksjons- og organisasjonsmyndighet.

## 2.3 Databehandler

I prosjektrapporten, SLA avtalen og den felles veilederen internkontroll og informasjonssikkerhet heter det at samarbeidsorganisasjonen ved daglig leder er databehandler for deltakerkommunene. I avsnitt 2.1 så vi at aktøren databehandler er aktuell når den behandlingsansvarlige setter ut behandlingsoppdrag til andre, også kjent som "outsourcing". Å fastslå hvorvidt samarbeidsorganisasjonen faktisk er å regne som databehandler er viktig. Loven stiller særskilte krav til bruk av databehandler og hvem som kan anses å være databehandler. I det følgende vil jeg først presentere de rettslige

---

organisert på det vi kan kalle et etats-/virksomhetsnivå underlagt rådmannen. Her finner vi skoler, barnehager, pleieinstitusjoner, helsetjeneste, teknisk tjenester osv.(Fimreite og Grindheim 2007:132).

[80] En ordfører kan tenkes å bli behandlingsansvarlig på kommunenes vegne dersom behandling av personopplysninger skjer under politisk ledelse.

[81] Datatilsynets årsmelding 2003:24

reguleringene vedrørende aktøren databehandler før jeg drøfter om samarbeidsorganisasjonen etter loven kan regnes som kommunenes databehandler. Hvis så er tilfellet må det også vurderes om forholdet mellom IKT- samarbeidet og deltakerkommunene er tilfredsstillende regulert etter loven.

### 2.3.1 Rettslige utgangspunkter

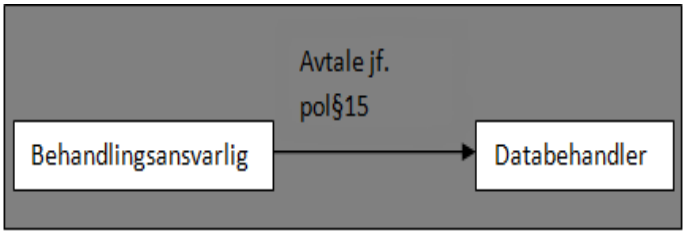
Databehandleren ble i kapittel 1.4.2 kort vist til som *den som behandler personopplysninger på vegne av den behandlingsansvarlige* jf. pol § 2 nr. 5. Definisjonen tilsvarer direktivets definisjon jf. art. 2, bokstav e:

*[…] den fysiske eller juridiske person, offentlige myndighet, byrå eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige[…]*

I likhet med pol sin definisjon av behandlingsansvarlig er også pol sin definisjon av databehandler mindre spesifikk enn i direktivet. Forarbeidene peker likevel på at selv om definisjonen er omformulert i forhold til direktivet, så skal innholdet anses å være det samme.[82]

Det er verken i direktiv, lov eller forskrift uttrykt eksplisitt at databehandler skal være en aktør utenfor den behandlingsansvarliges virksomhet. Det nærmeste en kommer i dette henseende er direktivets og lovens bruk av ” *på vegne av* den behandlingsansvarlige” og at det i forarbeidene vises til ”outsourcing.”[83] Uklarhetene omkring forståelsen av aktøren databehandler blir diskutert av Schartum og Bygrave.[84] De anfører at begrepet kan misforstås med den eller de personene som forestår den faktiske behandlingen av personopplysningene i den behandlingsansvarliges virksomhet og videre at bruken av begrepet i loven ikke direkte bidrar til å avkrefte en slik misforståelse (Schartum & Bygrave 2006:36). Dersom databehandleren hadde vært en del av den behandlingsansvarliges virksomhet ville dennes oppgaver kommet i form av instruksjon fra den behandlingsansvarliges ledelse.

Ved bruk av databehandler krever pol § 15 at det skal inngås en skriftlig avtale mellom partene. Av dette må en forstå det slik at




**Figur 7 ved bruk av databehandler skal det inngås en skriftlig avtale mellom partene jf pol § 15.**

[82] Ot. prp. nr. 92 (1998-99) s. 103
[83] Ot. prp. nr. 92 (1998-99) s.103
[84] Schartum & Bygraves Utredning av behov for endringer i personopplysningsloven 2006 kapittel 2.5.8.2

behandlingsansvarlig ikke har instruksjonsmyndighet ovenfor databehandleren. Hadde den behandlingsansvarlige hatt instruksjonsmyndighet ovenfor virksomheten som behandlet personopplysninger på sine vegne, hadde ikke avtale vært nødvendig og virksomheten ville ikke vært å anse som databehandler. Til tross for lovtekstens og direktivets uklarheter skal altså databehandler forstås som en ekstern aktør utenfor den behandlingsansvarliges virksomhet.[85] Coll og Lenth diskuterer ikke uklarhetene i loven direkte, men forutsetter på lik linje med Schartum og Bygrave at databehandleren ikke er i et ansettelsesforhold til den behandlingsansvarlige, men i et oppdragsforhold (Coll og Lenth 2000:36).

### 2.3.2 Spørsmål om hvorvidt IKT- samarbeidet er å anse som databehandler

Utgangspunktet her er at fire kommuner har gått sammen om et interkommunalt IKT – samarbeid. Som jeg redegjorde for i avsnitt 1.3.3 er noen av målene for samarbeidet å utvikle tjenesteproduksjon knyttet til administrative og publikumsrelaterte tjenester og å ivareta deltakerkommunenes oppgaver knyttet til drift, service og utvikling. Det er likevel slik at det på noen områder i deltakerkommunene finnes systemer som driftes av andre virksomheter enn samarbeidsorganisasjonen. Der det er snakk om behandling av personopplysninger må disse etter pol § 2 nr. 5 anses som databehandlere. Likevel vil ikke disse utenforstående aktørene bli vurdert i denne oppgaven. Det som er av interesse her er deltakerkommunenes forhold til samarbeidsorganisasjonen og at det er en dokumentert enighet mellom kommunene og samarbeidet at samarbeidsorganisasjonen er å anse som databehandler ovenfor deltakerkommunene.

Det mest vesentlige spørsmålet å stille for å slå fast hvorvidt samarbeidsorganisasjonen kan betegnes som databehandler er om den kan instrueres av kommunene. Etter samarbeidsorganisasjonens vedtekter er organisasjonen å regne som eget rettsubjekt. Dette peker i retning av at samarbeidsorganisasjonen er en ekstern virksomhet. Likevel er det flere faktorer som peker i motsatt retning. Etter vedtektene er det styret som har det administrative og organisatoriske ansvaret for driften av samarbeidet. Styret er sammensatt av rådmennene fra deltakerkommunene, bortsett fra kommune 1 som er representert ved assisterende rådmann. For tre av kommunene betyr dette at personen som er ansvarlig for å ivareta kommunens/den behandlingsansvarliges plikter også sitter i samarbeidsorganisasjonens styre. Videre i vedtektene heter det at styrets instruksjonsmyndighet er ubegrenset og at de kan

[85] For utfyllende drøfting av databehandler som aktør. Se Schartum & Bygraves Utredning av behov for endringer i personopplysningsloven 2006:36 flg.

delegere oppgaver til virksomhetens daglige leder og arbeidsutvalg. Dette betyr i teorien at det er et kollegium av rådmenn som etter vedtektene har instruksjonsmyndighet ovenfor resten av samarbeidsorganisasjonen.

I vedtektene kan man også lese at det er kommune 1 som har arbeidsgiveransvaret for samtlige arbeidstakere tilknyttet samarbeidsorganisasjonen. En kan anta at kommune 1 sitt arbeidsgiveransvar for samtlige ansatte i samarbeidsorganisasjonen innebærer at kommune 1 til syvende og sist også har instruksjonsmyndighet ovenfor de ansatte i samarbeidsorganisasjonen.[86]

Daglig leder for samarbeidsorganisasjonen fortalte i et intervju at det er de enkelte kommunene som selv bestemmer om det skal implementeres nye tjenester og det er også disse som gjør vedtak knyttet til budsjett og bevilgninger. Samarbeidsorganisasjonen sin oppgave i denne sammenheng er å bistå med faglig kompetanse i utredningsarbeid og å bidra med den faktiske iverksettingen av prosjekter og drift av nye tjenester. Samarbeidsorganisasjonen fremstår dermed mer som et saksforberedende organ ovenfor kommunene enn som en databehandler.

Det ble også forklart at samarbeidsorganisasjonens styre i dette henseende ikke har noen reel beslutningsmyndighet. De opptrer her som et koordinerende organ og bringer saker tilbake til det enkelte kommunestyret hvor selve myndighetsutøvelsen skjer.

Da vi snakket om samarbeidsorganisasjonens dokumenterte rolle som databehandler på vegne av kommunene ble det sagt at kommunenes og samarbeidsorganisasjonens forståelse av begrepet muligens ikke var helt i tråd med lovens definisjon. Et eksempel ble trukket frem: Før samarbeidet ble opprettet var IT-lederen i kommune 1 betegnet som databehandler på vegne av kommunen. Videre ble det fortalt at samme tankegang var lagt til grunn med samarbeidsorganisasjonen. Det betyr at selv om samarbeidsorganisasjonen regnes som en intern del av den enkelte kommune, har de selv valgt å konkludere med at de er databehandler ovenfor kommunene.

Som jeg var inne på i diskusjonen omkring databehandler- begrepet fremstår det som klart at en ansatt i kommunen eller en intern kommunal avdeling ikke vil være databehandler etter

[86] Utøvelse av en slik eventuell instruksjonsmyndighet vil trolig bryte med den underliggende avtalen om samarbeid mellom kommunene.

loven fordi denne personen eller denne avdelingen kan instrueres gjennom kommuneledelsens generelle instruksjons- og organisasjonsmyndighet.

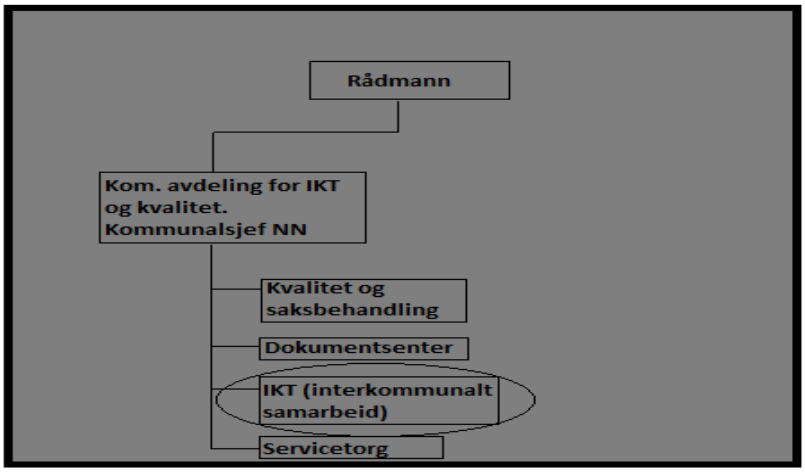
En rådgiver i samarbeidsorganisasjonen forklarte at de på egenhånd hadde valgt å definere seg som databehandler ovenfor kommunene. Han fortalte videre at dersom deres resonnement ikke var riktig, så var ansvars- og myndighetsforholdene godt regulert i SLA - avtalen og slikt sett var ikke deres eventuelle feilaktige tolkning av databehandlerbegrepet så viktig.

En virksomhetsleder i kommune 1 fortalte at samarbeidsorganisasjonen var en felles IKT-avdeling for de fire deltakerkommunene.

Rådmannen i kommune 2 viste til at samarbeidsorganisasjonen inngikk i kommunens organisasjonskart sammen med andre interkommunale samarbeid og i så måte ikke var en utskilt enhet. Ellers ble det gitt uttrykk for at samarbeidsorganisasjonen var å betrakte som kommunenes felles IKT- avdeling.

Rådmannen i kommune 3 uttrykte samme holdning som rådmannen i kommune 2. I kommune 3 hadde jeg også en samtale med en av kommunalsjefene. Da ble jeg fortalt at samarbeidet var – som et § 27 samarbeid, å betrakte som en intern avdeling i hver av deltakerkommunene.

Kommunalsjefen i kommune 4 understreket at det kun var kort tid siden de hadde gått inn i samarbeidet og at de kanskje ikke på nåværende tidspunkt hadde samme følelse av eierskap ovenfor samarbeidet som kommune 1, 2 og 3. På tross av dette ble samarbeidsorganisasjonen også her vurdert som en felles IKT- avdeling. Dette blir tydelig vist i kommunens organisasjonskart. Det interkommunale samarbeidet har her fått en egen plass under den organisasjonsgrenen som innebefatter kommunens arbeid med IKT.




Figur 8: Gjengivelse av kommune 4 sitt organisasjonskart. Her ser vi at det interkommunale samarbeidet fremstilles som en integrert del av kommunens avdeling for IKT og kvalitet.

På bakgrunn av kommune 1 sin status som arbeidsgiver ovenfor de ansatte i samarbeidsorganisasjonen og intervjuobjektenes beskrivelse av organisasjonen som en felles

og intern IKT- avdeling er det lite som tyder på at samarbeidet etter lovens definisjon kan være databehandler fordi, organisasjonen ikke direkte kan sies å være en ekstern aktør. Det er klart at organisasjonen utfører mange oppgaver som det hadde vært naturlig å legge til en databehandler, men formelt sett er det tvilsomt om de kan betegnes som databehandler. Samarbeidsorganisasjonen fremstår mer som et felles forum for diskusjoner som leder opp til lokal beslutningstaking. I dette tilfellet bidrar samarbeidsorganisasjonen med råd. Når beslutninger om implementering og valg av systemer blir tatt i den enkelte kommune, er det samarbeidsorganisasjonen som står for selve implementeringen og den påfølgende drift. Samarbeidsorganisasjonen blir dermed et saksforberedende og iverksettende organ. Det virker heller ikke som om samarbeidsorganisasjonen er særlig opptatt av at de eventuelt har mistolket begrepet databehandler og bruken av det. Det viktigste her, i følge dem selv, er hvordan de fordeler oppgaver mellom seg.

At samarbeidsorganisasjonen ikke er databehandler betyr at det ikke trenger å foreligge noen databehandleravtale etter pol § 15, likevel er det flere dokumenter i organisasjonen som tar sikte på å avklare spørsmål om de ulike aktørenes oppgaver, ansvar og roller. Dette må sies å være et godt og nødvendig tiltak. Med det sagt, vil det nok være fordelaktig for samarbeidsorganisasjonen og ikke bruke databehandlerbegrepet på den måten de gjør i dag. En feil bruk av begrepet kan skape uklarheter i ansvars- og myndighetsforhold og kan muligens skape forvirring i forhold til de aktører som etter personopplysningsloven faktisk vil være å anse som databehandlere for kommunene.

## 2.4 Avtaler mellom aktørene og oversikt over roller

Vi har sett at kommunene og samarbeidet selv har klassifisert samarbeidsorganisasjonen som databehandler, men at deres forståelse av begrepet ikke er forenelig med lovgivers. Dersom en gjør bruk av databehandler har det også blitt gjort klart at loven pålegger partene å inngå en skriftlig avtale. Uten databehandler kan en heller ikke kreve en databehandleravtale etter pol § 15. Til tross for at kravet om en databehandleravtale her faller bort, er det nok likevel viktig at det foreligger et avtaleverk mellom deltakerkommunene og samarbeidsorganisasjonen. Dette begrunnes i at en forutsetning for et vellykket samarbeid om informasjonssikkerhet er at ansvar og myndighet blir tydelig avklart. I og med at den enkelte kommune og samarbeidsorganisasjonen deler på oppgaver knyttet til gjennomføringen av informasjonssikkerhetsarbeidet, bør konkrete og dokumenterte avtaler mellom partene anses som nødvendig.

I det følgende vil jeg se nærmere på de rollene som er regulert i lov og forskrift og sammenligne dette med hvordan roller og ansvar er regulert i SLA- avtalen og kommunenes felles veileder for internkontroll og informasjonssikkerhet. Ved å gjøre dette vil vi få et bilde av hvordan kommunene og samarbeidsorganisasjonen samarbeider og hvorvidt deres organisering av informasjonssikkerhetsarbeidet tilfredsstiller lovens krav.  Jeg presenterer først de rollene som er angitt i lov og forskrift og deretter de ulovfestede rollene.

## 2.5 Den daglige ledelsen

### 2.5.1 Rettslige utgangspunkter

Forskriftens § 2-3, første ledd angir rollen daglig leder. Her fremgår det at den som utgjør den daglige ledelsen i den behandlingsansvarliges virksomhet som har ansvaret for at reglene i pof kapittel 2 følges.

Det kan i utgangspunktet være usikkert akkurat hvem som skal bekle denne rollen og forskriften tilbyr selv ingen klar *definisjon* av begrepet (Haug 2006:145), men av ordlyden må vi forstå at rollen er tiltenkt en bestemt person.

Forskriften regulerer eksplisitt kun det rettslige ansvaret for den daglige ledelsen i den behandlingsansvarliges virksomhet. Schartum peker på at et slikt ansvar også må ligge hos daglig ledelsen hos en eventuell databehandlers virksomhet (Schartum 2005:112). I dette henseende kan en tenke seg at daglig leder for den behandlingsansvarliges virksomhet først og fremst skal fokusere på arbeidet innenfor sin virksomhet og samtidig styringen av

databehandleren gjennom avtaleverk. Den daglige ledelsen av databehandlerens virksomhet skal primært jobbe innenfor avtalens rammer og forestå den daglige driften og behandlingen av personopplysningene (ibid.). Selv om samarbeidsorganisasjonen i dette tilfellet ikke er databehandler, vil det nok være hensiktsmessig for samarbeidet at daglig leder her også tar på seg et ansvar for å ivareta bestemmelser knyttet til informasjonssikkerhet. Dette begrunnes ut i fra det faktum at kommunene og samarbeidsorganisasjonen deler på rettslige plikter etter pof. Dette blir videre behandlet i avsnitt 2.5.4.

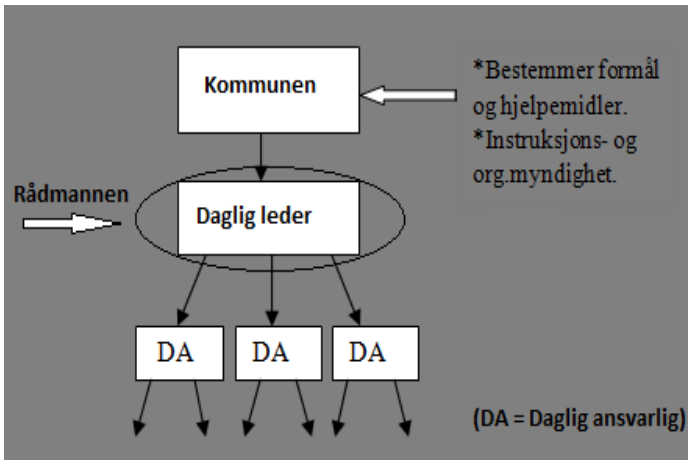
### 2.5.2 Drøftelse av daglige ledere i kommunene

Når det gjelder kommuner kunne vi av bestemmelsens ordlyd tenkt oss at dette enten er ordføreren - fordi han/hun er kommunens rettslige representant etter kommuneloven § 9, eller rådmannen som etter kommuneloven § 23 nr.1 er øverste leder for administrasjonen. Vi har sett at alle kommunene som inngår i caset har tillagt kommunen ved sine rådmenn behandlingsansvaret og av dette kan vi slutte at ordføreren i denne omgang faller utenfor diskusjonen.

Schartum og Bygrave antyder at den daglige ledelsen er den som er øverste operative leder for en virksomhet (Schartum & Bygrave 2006:34). Datatilsynet har påpekt at de i praksis ikke forventer at rådmannen - eller øverste leder i en annen type virksomhet, skal ha inngående kunnskap om informasjonssikkerhet, men de framholder at ansvaret for at opplysninger blir sikret på en forsvarlig måte er hans/hennes ansvar.[87] Rådmannen kan delegere den operative kompetansen og/eller daglige arbeidsoppgaver knyttet til informasjonssikkerhet. I den grad den enkelte rådmann ikke har særlig inngående kunnskap om regelverket eller er spesielt opptatt av sikkerhetsarbeid, må dette anses å være hensiktsmessig. Med det sagt kan man anta at det for kommuner som hovedregel vil være rådmannen som har den daglige ledelsen av den behandlingsansvarliges virksomhet og dermed også har ansvaret for at bestemmelsene i kapittel 2 blir etterlevd. Adgangen til delegasjon gjør imidlertid at den enkelte rådmann ikke nødvendigvis har en særlig operativ rolle i informasjonssikkerhetsarbeidet, men det er ikke særlig tvil om at ansvaret ved brudd vil ligge hos han/henne.

[87] Datatilsynets veileder om internkontroll og informasjonssikkerhet 2009:3 (se for øvrig Coll & Lenth 200:36)

Hos kommunene i caset ser det ut til at alle har en felles forståelse av at det er rådmannen i den enkelte kommune som er daglig leder med det ansvaret dette innbærer etter pof § 2-3 første ledd. Dette er også bekreftet i SLA avtalen som slår fast at det er den enkelte kommunes rådmann som er hovedansvarlig for kommunens forpliktelser ovenfor pol.




Figur 9 Den daglige lederen for den behandlingsansvarliges virksomhet (Kommunene) er i dette tilfellet rådmannen i den enkelte kommune.

Samtidig ser det ut til at ingen av rådmennene spiller en særlig aktiv rolle når det kommer til det operative arbeidet. Da representanter fra deltakerkommunene og samarbeidsorganisasjonen ble spurt om hvem som hadde det overordnede ansvaret for kommunens plikter i forhold til personopplysningsloven var de alle samstemte.
I kommune 1 snakket jeg med en virksomhetsleder. Han viste til at det var rådmannen i kommunen som var den øverste ansvarlige. Dette var etter hans oppfatning godt forankret i kommunen.

I kommune 2 snakket jeg med rådmannen. Han erkjente at han selv ikke hadde inngående kunnskap om regelverket i pol eller pof, men han var klar over at det var han som var ansvarlig "hvis noe gikk galt". Ut over dette preget ikke denne type spørsmål hans arbeidshverdag.

I kommune 3 intervjuet jeg kommunens rådmann. Han erkjente at han selv ikke hadde inngående kunnskap om regelverket i pol eller pof, men var klar over at han var den med det overordnede ansvaret for behandling av personopplysninger i kommunen. Han utdypet videre at alle oppgaver knyttet til dette ansvaret var delegert nedover i organisasjonen.

I kommune 4 intervjuet jeg kommunalsjefen som fortalte at det var rådmannen som hadde det overordnede ansvaret i forhold til personopplysningsloven, mens det daglige arbeidet med sikkerhet var lagt til henne. I denne kommunen var det en egen avdeling som jobbet med IKT, sikkerhet og beredskap. Kommunalsjefen kunne fortelle at rådmannen i kommunen var veldig klar på at ivaretakelse av interesser som gjaldt personvern og informasjonssikkerhet var

viktige saker på agendaen og at initiativet til å bedre på disse forholdene i kommunen i utgangspunktet hadde kommet fra rådmannen selv.

Det synes klart at alle deltakerkommunene er innforstått med at rådmannen har det overordnede ansvaret for den enkelte kommunes ivaretakelse av regelverket i pol og pof. Likevel er det slik at rådmennene selv - muligens med unntak av rådmannen i kommune 4, er lite direkte involvert i arbeidet. Dette kan betraktes som en svakhet. Datatilsynet har uttalt at spørsmål knyttet til informasjonssikkerhet (og internkontroll) er et ledelsesansvar. Som vi så i avsnitt 1.4.2 bygger regelverket omkring informasjonssikkerhet blant annet på prinsippet om ledelsesstyring. Med dette menes det at prosesser omkring personvern og informasjonssikkerhet skal løftes opp på det øverste administrative nivået. Tanken er at forankring hos ledelsen vil bidra til at informasjonssikkerhet kommer på kommunenes sakskart og at medarbeidere nedover i systemet oppfatter dette arbeidet som viktig (Tranvik 2009:23). I kommunene som har blitt studert her ser det likevel ut til - med unntak av kommune 4, at selv om alle rådmennene er klar over sitt ansvar, så er de ikke særlig personlig involvert i arbeidet med informasjonssikkerhet, og gjør heller ikke mye for å sette dette på dagsorden. Med tanke på rådmennenes sentrale posisjon i samarbeidsorganisasjonen er dette overraskende og foruroligende. Styret i samarbeidsorganisasjonen har vedtatt at felles retningslinjer for informasjonssikkerhet skal gjelde, likevel ser ikke dette vedtaket ut til å ha økt den enkelte rådmanns oppmerksomhet på utfordringene med å oppnå en tilfredsstillende sikring av personopplysninger.

En kan muligens argumentere for at selv om den enkelte rådmann ikke er aktiv i det daglige arbeidet, så viser vedtaket om utarbeidelse av veilederen at informasjonssikkerhet i hvert fall er satt på dagsordenen. I hvilken grad en kan snakke om god forankring er likevel noe uklart. I Tranvik sine studier av informasjonssikkerhet i norske kommuner kom det frem at en hemmende faktor vedrørende organiseringen av sikkerhetsarbeidet var manglende interesse og forankring på rådmannsnivå (Tranvik 2009:93). Vi har og sett at Datatilsynet ikke krever eller forventer at rådmannen som daglig leder skal ha inngående kunnskap om informasjonssikkerhet. Det han/hun på den annen side skal ha, er en visshet om at grunnlaget for forsvarlig sikkerhet er til stede (Leif T. Aanensen 2008:25). Med vedtaket om å utarbeide felles retningslinjer for internkontroll og informasjonssikkerhet kan en si at de har tatt et steg i riktig retning, men det betyr ikke at rådmannens jobb er gjort. Rådmannen må som daglig leder følge opp retningslinjene og sørge for at innholdet i disse blir ivaretatt.

I forbindelse med at rådmennene i dette caset har en begrenset pratisk rolle når det gjelder informasjonssikkerhetsarbeidet kan en muligens diskutere om rollen *den med den daglige ledelsen* skal "flyttes" et nivå ned i hierarkiet, til virksomhetsledere. Slik det står seg i dag er oppgaver knyttet til rollen som den med den daglige ledelsen delegert fra rådmann til virksomhetsledere, men ansvaret ligger fortsatt hos rådmannen. Kanskje en bør diskutere hvorvidt virksomhetsledere eller mellomledere i større grad bør gjøres ansvarlig for de behandlingene som skjer innenfor deres virksomhet.

Pof § 2-3 gir den med daglige ledelsen ansvar for å påse at "*formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål."*[88] I tillegg skal all bruk av informasjonssystemer *jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.*[89]

Som jeg pekte på innledningsvis er kommuner i seg selv relativt komplekse organisasjoner (avsnitt 1.3.3). Det blir foretatt mange ulike behandlinger innenfor en kommunes forskjellige virksomheter. Dermed blir rådmennene som øverste ansvarlig på kommunens vegne nærmest overøst med behandlingsansvar, og en kan stille spørsmålstegn ved om rådmenn skal være "blindt" ansvarlig for alle disse behandlingene. Det å flytte den daglige ledelsen til virksomhetsledere kan kanskje være hensiktsmessig i og med at disse muligens har bedre kunnskap om de behandlingene som foretas innenfor sitt virksomhetsområde og bedre kan kontrollere om reglene om informasjonssikkerhet blir fulgt og at man i større grad har kompetanse til å vurdere personopplysningslovens - og forskriftens sikkerhetskrav opp mot særlover innenfor spesifikke virksomhetsområder.

### 2.5.4. Daglig leder i samarbeidsorganisasjon

Forskriften regulerer bare eksplisitt sikkerhetsansvaret for en daglig leder i den behandlingsansvarliges virksomhet. Schartum påpeker at en implisitt må forstå at et tilsvarende ansvar må plasseres hos en eventuell databehandler (Schartum 2005:112). Riktignok er ikke samarbeidsorganisasjonen databehandler, men organisasjonen har like fullt oppgaver knyttet til informasjonssikkerhet. Så lenge samarbeidsorganisasjonen har sine

[88] Pof § 2-3 andre ledd.
[89] Pof § 2-3 fjerde ledd.

konkrete oppgaver og er fysisk utskilt fra deltakerkommunene, vil det derfor være naturlig at den daglige lederen for samarbeidsorganisasjonen tar et visst ansvar for de delene av informasjonssikkerhetsarbeidet som foregår i deres organisasjon. Daglig leder i samarbeidsorganisasjonen virket inneforstått med at han hadde et slikt ansvar, men det var i hovedsak driftsavdelingen og prosjekt- og utviklingsavdelingen som hadde daglige oppgaver knyttet til informasjonssikkerhet (se forøvrig avsnitt 2.6.3)

## 2.6 Den med det daglige ansvaret

### 2.6.1 Rettslige utgangspunkter

Den med det *daglige ansvaret* blir nevnt i forbindelse med pol § 18, første ledd bokstav b. Ved innsynsbegjæring har en blant annet rett til å få vite hvem som har det daglige ansvaret for at den behandlingsansvarliges plikter blir oppfylt. I tillegg skal det i en *virksomhets melding til Datatilsynet* fremgå hvem som har det daglige ansvaret for å oppfylle den behandlingsansvarliges plikter jf. pol § 32 første ledd, bokstav c. Forarbeidene utdyper denne rollen noe:

*Ledelsen må sørge for at loven etterleves, og som ledd i dette foreta en intern arbeidsfordeling slik at det er klart hvilken stilling det ligger til å sørge for at loven etterleves i praksis.*[90]

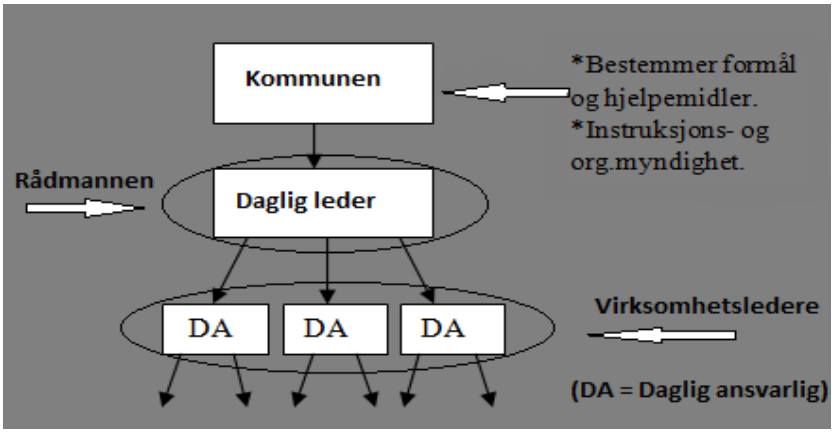
Dette utsagnet blir i forarbeidene videre koplet til pol § 18 bokstav b. Som vi så over, er dette et krav om at behandlingsansvarlig ved forespørsel skal kunne oppgi hvem som har det daglige ansvaret. Til tross for at adgangen til intern arbeidsfordeling er relativt fri, bør den som blir tildelt det daglige ansvaret være en person i en lederstilling. Dette begrunnes i at den som får rollen bør ha en reell innflytelse på behandlingene som foretas.[91] Hos samtlige kommuner som studeres her, er det daglige ansvaret delegert fra rådmannen til andre.

[90] Ot. prp. nr 92 (1998-99) s. 102
[91] Ot. prp. nr 92 (1998-99) s. 102

### 2.6.2 Drøftelse av daglig ansvarlige i kommunene

Tidligere har jeg vært inne på at delegasjon og en intern arbeidsfordeling nærmest er en nødvendighet for å få til et godt arbeid vedrørende sikring av personopplysninger. Dette har også blitt gjort i alle kommunene i caset.

I SLA- avtalen og i den felles veilederen vises det til en rolle som systemeier (avsnitt 2.9.2). I følge dokumentasjonen er det systemeieren som har det daglige ansvaret for at kravene til sikring av personopplysninger blir etterlevd innenfor sin virksomhet.




Figur 10 Den med det daglige ansvaret er som regel virksomhetslederne i den enkelte kommune.

I kommune 1 er det virksomhetsledere som i all hovedsak er definert som systemeiere og som har det daglige ansvaret for at pol og pof sine bestemmelser blir fulgt. Innenfor helse og omsorg er det daglige ansvaret løftet opp et nivå, til en kommunalsjef. Dette begrunnes i at det innenfor denne sektoren er sektorovergripende fagsystemer.

I kommune 2 er denne rollen i følge rådmannen tildelt den enkelte virksomhetsleder, men tilføyer at det praktiske arbeidet knyttet til det å være systemeier ved noen anledninger er delegert til en annen innenfor den enkeltes virksomhetsleders virksomhet.

I kommune 3 er det løst på samme måte, den enkelte virksomhetsleder har blitt tildelt systemeier -rollen innenfor de fagsystem som ligger under hans eller hennes virksomhet. I følge kommunens rådmann er dette klart definerte roller og de er dokumenterte.

I kommune 4 er det løst på samme måte som hos de andre. Innenfor skole samt helse og omsorg er det to forskjellige kommunalsjefer som har systemeier- rollen.

I alle kommunene virket begrepet systemeier å være godt innarbeidet og mer brukt enn *den med det daglige ansvaret.* Etter SLA- avtalen og den felles veilederen blir systemeier også beskrevet som den som etter pol og pof har det daglige ansvaret for å ivareta den behandlingsansvarliges forpliktelser innenfor sin virksomhet. Den med det daglige ansvaret er

altså i all hovedsak virksomhetsledere eller kommunalsjefer. Dette betyr at ansvaret er lagt til en person i en lederstilling som gjør at den med det daglige ansvaret har reell innflytelse.

I forbindelse med diskusjonen på tampen av avsnitt 2.5.2, hvor jeg foreslo at virksomhetsledere kunne bli tildelt rollen som *den med den daglige ledelsen,* ville det i forlengelse av den tanken vært naturlig at rollen som den med det daglige ansvaret ble flyttet til de som i dag er systemansvarlige og underordnet virksomhetsleder/systemeier (se for øvrig avsnitt 2.9.3).

### 2.6.3 Daglig ansvar i samarbeidsorganisasjonen

På lik linje med rollen som daglig leder, må vi forstå at også rollen som daglig ansvarlig bør ha en ekvivalent i samarbeidsorganisasjonen. Ser vi til SLA- avtalen finner vi noen roller som ikke er regulert i pol eller pof, men som kan angi rollen som daglig ansvarlig på samarbeidsorganisasjonens side. Avtalen opererer med koordineringsansvarlig og driftsansvarlig. Rollen som koordineringsansvarlig beskrives i dokumentet som samarbeidets kontaktperson for systemeier og systemansvarlig i den enkelte kommune, oppgavene til denne personen handler imidlertid mer om rådgivning, ansvar for oppdateringer/oppgraderinger og å bistå med best mulig utnyttelse av de ulike system. Det er rollen som driftsansvarlig som er mest interessant i dette henseende. Driftsansvarlig har (etter avtalen):

- Ansvar for at den tekniske driften av systemet er i henhold til gjeldende lovverk og retningslinjer for IT-sikkerhet.
- Ansvar for at oppgradering og drift av system er forsvarlig og i samsvar med gjeldende lover og forskrifter.

Ut i fra dette kan den driftsansvarlige ses på som den i samarbeidsorganisasjonen som har daglig ansvar for det eller de fagsystemer som han eller hun drifter.

## 2.7 Sikkerhetsrevisor(er)

### 2.7.1 Rettslige utgangspunkter

Denne rollen er beskrevet i forskriften § 2-5 som krever at det skal gjennomføres sikkerhetsrevisjon. Det stilles ingen direkte krav om at revisjonen skal utføres av eksterne aktører, men i tråd med hva man i dagligspråket forstår med revisjon, så må en kunne stille krav om at den som utfører revisjonen opptrer med en viss integritet og uhildethet.  Det er den daglige lederen som skal påse at denne revisjonen finner sted (jf. ovenfor) og ved bruk av

databehandler må regelverket forstås slik at det også i den virksomheten skal foretas sikkerhetsrevisjoner.

### 2.7.2 Drøftelse av sikkerhetsrevisor i kommunene og i samarbeidsorganisasjonen

Verken i SLA avtalen eller i den felles veilederen nevnes sikkerhetsrevisor som en egen rolle. Vi har sett at det er den med det daglige ansvaret som har ansvaret for at kommunenes plikter etter pol blir ivaretatt innenfor sitt virksomhetsområde. Dette bør innebære at det innenfor hver virksomhet finnes en person som har ansvar for revidering av virksomhetens sikkerhetsrutiner. I den felles veilederen slås det fast at det er den enkelte systemeier som er ansvarlig for at det minimum en gang i året gjennomføres sikkerhetsrevisjon. At ansvaret for gjennomføring av revisjon er tillagt systemeier er i utgangspunktet uproblematisk. Det viktigste må være at revisjonen faktisk skjer. Spørsmålet er derfor om det gjennomføres revisjon og om dette gjøres av systemeier selv eller om oppgaven er delegert til noen andre innenfor virksomheten.

Da jeg spurte representanter fra den enkelte kommune om de hadde en person som jobbet spesielt med revisjon knyttet til informasjonssikkerhet og behandling av personopplysninger var svarene fra kommunene 1 og 3 nei. Dette var en oppgave som var tillagt systemeier.

I kommune 2 ble jeg henvist til kommunens beredskapskoordinator. Beredskapskoordinatoren hadde ansvar for revisjon av kommunens beredskapsplanverk og risikovurderinger knyttet til dette. Han sa imidlertid at han ikke drev med revisjon av rutiner knyttet til sikring av personopplysninger, men delvis revisjon av vurderinger knyttet til IKT. Når det gjaldt revisjon av rutiner knyttet til revisjon av behandling av personopplysninger ble jeg henvist til den enkelte virksomhetsleder.

I kommune 4 stilte det seg noe annerledes. Selv om det også var den enkelte systemeier som hadde det formelle ansvaret for at revisjon av rutiner ble gjennomført hadde kommunen en mer sentralisert styring av sine informasjonssikkerhetsrutiner. De hadde en egen avdeling som jobbet med IKT og beredskap. Her var det en kommunalsjef som jobbet med et felles system for revisjon.

I samarbeidsorganisasjonen har vi sett at det finnes en driftsansvarlig. I følge veilederen er det denne personen som er ansvarlig for å drifte de ulike systemene etter avtale med systemeier. Der sikkerhetsrevisjoner på kommunesiden dreier seg om revisjon av juridisk karakter, kan sikkerhetsrevisjoner som gjennomføres i samarbeidsorganisasjonen sies å være av teknisk

karakter. Den driftsansvarlige har ansvar for at de ulike systemene driftes i henhold til gjeldende lovverk og retningslinjer for IT-sikkerhet. Og i og med at kommunenes IT-infrastruktur driftes sentralt er det naturlig at de tekniske elementene av sikkerhetsrevisjoner foregår her.

## 2.8 Personell og brukere av informasjonssystemer som behandler personopplysninger

### 2.8.1 Rettslige utgangspunkter

Denne rollen omhandler *personellet* i den behandlingsansvarliges virksomhet og deres ansvar. Dette blir regulert i pof §§ 2-8 og 2-9. Pof § 2-8 slår fast at ansatte i en virksomhet som har befatning med informasjonssystemer som behandler personopplysninger skal være autoriserte for bruk av de systemene og at bruken skal begrenses til det som er tjenstlig nødvendig (Johansen et al. 2001:351). Av dette forstår man at ansatte/brukere må få tilstrekkelig opplæring med tilknytning til internkontroll, informasjonssikkerhet, den enkeltes juridiske ansvar, sikringstiltak og riktig bruk av aktuelle informasjonssystemer.[92] Bestemmelsen kan likevel ikke tolkes slik at ansattes private bruk av informasjonssystemet er forbudt, men privat bruk bør ikke forekomme dersom personopplysninger hos den behandlingsansvarlige blir utsatt for ytterligere risiko (Johansen et al. 2001:352).

Pof § 2-9 omhandler taushetsplikt. Her legges det særlig vekt på at medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt der behov for konfidensialitet er nødvendig. Pof § 2-9, siste setning påpeker at taushetsplikten også gjelder annen informasjon som er av betydning for informasjonssikkerheten. Dette kan for eksempel være informasjon om det enkelte informasjonssystem der behandling av personopplysninger foregår. I avsnitt 1.4.3 drøftet jeg kort forholdet mellom pol og taushetsplikt- bestemmelsen i fvl § 13. I denne oppgaven er det kommunal sektor som studeres og derfor må en være klar over at ansatte i offentlige forvaltningsorgan er pålagt en generell taushetsplikt.[93] Videre vet vi at det også finnes sær- regler som stiller krav til taushetsplikt, disse må da sammenholdes og evalueres opp mot reglene i pof § 2-9 og fvl § 13.[94] I likhet med de andre rollene jeg har presentert må man anta at tilsvarende føringer også må tillegges øvrige ansatte/personell hos databehandleren, dersom den behandlingsansvarlige gjør bruk av en slik.

[92] Datatilsynets veileder om internkontroll og informasjonssikkerhet 2009:39
[93] Se fvl § 13
[94] Eksempel på slike regler er helsepersonelloven § 21flg og sosialtjenesteloven§ 8-8.

### 2.8.2 Om Ansatte i kommunene og ansatte i samarbeidsorganisasjonen

SLA avtalen presiserer at alle brukere som benytter seg av systemer som på en eller annen måte er relatert til behandling av personopplysninger, skal følge gjeldende rutiner for bruk av informasjonssystemene og videre at alle brukere skal melde fra om avvik når det er nødvendig. Den felles veilederen sier det samme. Med benevnelsen "*alle brukere"* må det forstås at dette ikke bare gjelder for eksempel saksbehandlere i kommunene, men også andre personer som har sitt virke i samarbeidsorganisasjonen.

## 2.9 Roller som ikke er rettslig regulert.

Over har jeg gått gjennom de rollene som eksplisitt eller implisitt er regulert i pol og pof. Ved studier av caset dukket det også opp noen andre rollebetegnelser som samarbeidet og kommunene har definert på egenhånd. I den forbindelse er det viktig å gjøre noen avklaringer opp mot de rollene som er definert i lov og forskrift. Dette er særlig viktig der en person har en rolle definert etter lov og en annen rolle definert av samarbeidet og kommunene selv. Slike avklaringer er også viktig for å rydde opp i eventuelle kilder til forvirring. Dersom det er uklart hvilke rolle(r) en ansatt har, kan dette påvirke organiseringen av informasjonssikkerhetsarbeidet og gjennomføringen av oppgavene som den enkelte person er ansvarlig for. Rollene som presenteres nedenfor er alle sentrale i kommunenes og samarbeidsorganisasjonens arbeid med ivaretakelse av informasjonssikkerhetsarbeid.

### 2.9.1 Sikkerhetsansvarlig

Rollen som sikkerhetsleder eller sikkerhetsansvarlig er ikke direkte regulert i lov, forskrift eller forarbeider.  I Datatilsynets veiledningsmateriell benevnes likevel rollen som sikkerhetsansvarlig som viktig. I avsnitt 2.5 flg. så vi at det er den enkelte rådmann – som utgjør den daglige ledelsen, som har ansvaret for at bestemmelsene i forskriftens kapittel 2 følges. Rollen som sikkerhetsansvarlig er tiltenkt en person som avlaster den daglige ledelsen og som rapporterer direkte til rådmannen. Rådmannen vil alltid ha det formelle og reelle ansvaret, men den sikkerhetsansvarlige vil ha en gjennomførende og koordinerende rolle når det gjelder kommunens helhetlige sikkerhetsarbeid.

Datatilsynet har utarbeidet en egen veileder for en sikkerhetsansvarlig.[95] Det er viktig å presisere at denne malen muligens går noe utover lovens minimumskrav og at den må tilpasses den enkelte virksomhet ut i fra størrelse og omfang vedrørende behandling av personopplysninger. Kjerneoppgavene til en sikkerhetsansvarlig vil være å ha en

[95] Veileder tilgjengelig på www.datatilsynet.no 2-19_sikkerhetsintruks_sikkerhetsansvarlig

koordinerende rolle og sørge for å opprette og gjennomføre regime for internkontroll og informasjonssikkerhet. Herunder å påse at de enkelte avdelinger/ansatte i virksomheten gjennomfører plikter etter lov og forskrift på en tilfredsstillende måte.

Ledelsen i det interkommunale IKT- samarbeidet har tatt til orde for at det skal etableres en sikkerhetsansvarlig i hver kommune og at dennes oppgaver blant annet skal bestå av å godkjenne større endringer av infrastruktur og programvare, ajourhold over den enkelte kommunes informasjonssystemer i samråd med samarbeidsorganisasjonen, motta og følge opp sikkerhetsrevisjoner fra systemeiere, årlig arrangere sikkerhetsforum og årlig følge opp ledelsens gjennomgang i henhold til fastlagte prosedyrer. Jeg kommer tilbake til sikkerhetsansvarlige i den enkelte kommune i avsnitt 3.1.2.

### 2.9.2 Systemeier

Det interkommunale IKT- samarbeidet operer med betegnelsen systemeier. Innenfor IT-litteratur blir denne betegnelsen ofte brukt om den eller de personene som har det formelle eierskapet over en dataressurs, som for eksempel en database eller maskinvare (Daler et al. 2006:459). Denne forståelsen av begrepet kan peke mot at det er en virksomhets øverste ledelse som i utgangspunktet er systemeier. Samarbeidsorganisasjonen har tolket begrepet noe annerledes. Systemeier brukes her om den person som har det øverste ansvaret for et fagsystem innenfor sitt virksomhetsområde. I forhold til bestemmelsene vedrørende informasjonssikkerhet vil rollen som systemeier i dette tilfellet ligge til samme person som har det daglige ansvaret for å ivareta den behandlingsansvarliges plikter etter pol og pof. Dette kommer også frem i avtaleverket mellom samarbeidsorganisasjonen og kommunene hvor det heter at *"systemeier har […] daglig ansvar for å oppfylle plikter som behandlingsansvarlig på vegne av rådmannen jf. personopplysningsloven og retningslinjer for IKT- sikkerhet"*. Se for øvrig avsnitt 2.6.1 flg.

### 2.9.3 Systemansvarlig

Systemansvarlig ligger hierarkisk under systemeieren. Det interkommunale IKT- samarbeidet definerer systemansvarlig *som den som har det faglige ansvaret for bruk og administrasjon av systemet*. Arbeidsoppgaver som følger denne rollen er blant annet å være kontaktperson mot samarbeidsorganisasjonen og deres brukerstøtte. I denne rollen ligger også oppgaver direkte knyttet til informasjonssikkerhet. Blant annet er det den systemansvarlige som skal styre brukertilgang og etablere og dokumentere rutiner som er nødvendige for bruk av systemet. I

følge avtaleverket kan systemansvarlig også på bestilling fra systemeier utføre systemeieroppgaver.

### 2.9.4 Driftsansvarlig

Rollen som driftsansvarlig er i avtaleverket mellom kommunene og samarbeidsorganisasjonen definert som *en som er ansvarlig for å drifte systemer etter avtale med systemeier*. Det som er spesielt i dette tilfellet er at alt driftspersonell er flyttet ut av den enkelte kommune og jobber for samarbeidsorganisasjonen i deres felles lokaler. Den driftsansvarlige har flere oppgaver som er knyttet til informasjonssikkerhet, herunder: Å bidra til avviksrapportering, innhente godkjennelse fra systemeier før tekniske endringer utføres og å påse at gjeldende tekniske og administrative driftsrutiner blir fulgt.

## 2.10 Samlet vurdering av aktører og roller

Ovenfor har jeg gått igjennom de rollene som er definert eksplisitt og implisitt i pol og pof. I tillegg har jeg presentert noen roller som er definert og dokumentert hos kommunene og samarbeidsorganisasjonen. Vi har sett at samarbeidsorganisasjonen selv har valgt å definere seg som databehandler, men at de etter loven neppe kan betegnes som databehandler. Til tross for at samarbeidsorganisasjonen ikke er databehandler vil jeg videre i oppgaven betegne også dem som en aktør fordi de er en egen avdeling med egne oppgaver relatert til informasjonssikkerhet på deltagerkommunenes vegne.

Dersom en skal stille spørsmål om hvorvidt casets bruk og organisering av roller er i tråd med lovgivningen, er det flere momenter som kan gjøre det utfordrende å konkludere her.

Alle kommunene har definert rådmannen som behandlingsansvarlig på vegne av sin kommune. Videre har alle deltakerkommunene definert systemeiere for sine fagsystemer og denne rollen tilsvarer den med det daglige ansvaret (avsnitt 2.6). Kommunene har også definert systemansvarlige og disse ligger direkte under systemeier. Her kommer det frem at kommunene og samarbeidsorganisasjonen har brukt andre begreper enn de som finnes i lov og forskrift. Det blir stilt likhetstegn mellom systemeier og daglig ansvarlig og rollen som systemansvarlig har blitt tildelt en del oppgaver knyttet til sikkerhet.

Jeg har også vist til rollene sikkerhetsrevisor og sikkerhetsansvarlig. Ingen av kommunene har en egen person med fast ansvar for revisjon av sikkerheten. Det ser heller ikke ut til at dette kommer til å bli opprettet i nærmeste fremtid. Likevel har vi sett at det den enkelte systemeier er tillagt noen revisjonsoppgaver, selv om disse er vagt regulert i de felles retningslinjene.

Rollen som sikkerhetsansvarlig er per i dag heller ikke opprettet i kommunene, men dette jobbes det med i disse dager (se for øvrig avsnitt 3.1)

Skal en påpeke feil og mangler i deres dokumentasjon vil jeg først og fremst trekke frem at bruken av databehandlerbegrepet er noe misforstått. Jeg vil også trekke frem en noe løs dokumentering av revisjonsansvar og fraværet av sikkerhetsansvarlige i kommunene. Hvorvidt sistnevnte preger kommunenes og samarbeidets arbeid med informasjonssikkerhet vil bli drøftet i kommende kapittel.

Samarbeidsorganisasjonen på sin side har klargjort hvem som har rollene som driftsansvarlige. Dette er eksplisitt dokumentert i samarbeidsorganisasjonen og alle systemeiere i den enkelte kommune vet hvem som er driftsansvarlig for det systemet/systemene de har ansvar for. Kommentarene til forskriften presiserer at det er særlig viktig at ansvar og myndighet relatert til driftsledelse (hvem som skal ha en *operasjonell* rolle) og sikkerhetsledelse (hvem som skal ha en kontroll- rolle) blir klarlagt. Disse rollene bør i følge kommentarene legges til to ulike stillinger i virksomheten, men som vi skal se er ikke dette alltid mulig eller nødvendig (Johansen et. al 2001:350). I tilfellet med deltakerkommunene og samarbeidsorganisasjonen skal vi se at drift og kontroll er delt mellom aktørene. Vi har sett at driftsansvaret ligger hos ansatte i samarbeidsorganisasjonen og at det for tiden jobbes mot etablering av en sikkerhetsansvarlig (den operasjonelle rollen) i den enkelte kommune. Slikt sett møter man oppfordringen i kommentarutgaven om at disse rollene skal ligge til to ulike personer. Om dette vil ha noen innvirkning på samarbeidet at disse to rollene vil være fysisk adskilt ved at de ligger i to ulike virksomheter og hvorvidt denne rolleinndelingen påvirker måten kommunene og samarbeidet løser sine oppgaver på vil være tema i neste kapittel.

Et annet moment når en skal diskutere om casets organisering av roller og fordeling av ansvar er i tråd med loven, er at lov og forskrift i dette tilfellet ikke regulerer interkommunale samarbeid direkte. Det kan dermed være vanskelig å vurdere hvordan man skal fordele roller og ansvar i et samarbeid der flere er behandlingsansvarlige, daglige ledere, daglig ansvarlige og hvor IKT- ressursene er sentralisert. I denne forbindelse kan det være aktuelt å diskutere om lovgiver og/eller forskriftmyndighet skal vurdere om de kan bidra med avklaringer i form av bestemmelser om ansvar, myndighet og oppgavedeling. Samme spørsmål kan rettes mot Datatilsynet og KS. Kan Datatilsynet som tilsynsmyndighet/rådgivende organ og KS som

interesseorganisasjon bidra med råd og veiledning som forenkler arbeid med informasjonssikkerhet i interkommunale samarbeid?

## 3 Gjennomføring og organisering av sikkerhetsarbeidet

Vi har sett hvordan loven stiller krav til avklaring av ansvars og myndighetsforhold og viktigheten av en bevisst og strukturert arbeidsfordeling. Vi har sett hvilke rettslige og ikke-rettslige regulerte roller som inngår i arbeidet med informasjonssikkerhet, samt reguleringen av deltakerkommunenes forhold til samarbeidsorganisasjonen. Når de ulike rollene er avklart blir det viktig å se på hvilke konkrete organisatoriske oppgaver som ligger til den enkelte kommune og hvordan personene i de ulike rollene deltar her. Dokumentasjonskravene er omfattende. Blant annet skal hver kommune ha beskrivelser av sikkerhetsmål og strategi.[96] Det skal etableres rutiner for risikovurderinger, revisjoner og avvikshåndtering.[97] I det følgende presenterer jeg ulike rettslige krav for gjennomføring av sikkerhetsarbeidet. Videre knyttes disse kravene opp til rollene som er presentert i kapittel 2. Det vil også bli interessant å se om den interkommunale samarbeidsorganisasjonen har tatt på seg noen av de rollene og oppgavene som normalt ville ligget hos den enkelte kommune, og på den måten påvirker deltakerkommunenes arbeid med informasjonssikkerhet.

2. I hvilken grad er den dokumenterte ansvars- og myndighetsfordelingen ivaretatt i praksis?

    a. Utfører de ulike aktørene de oppgaver de er pålagt etter avtaleverket?
    b. I hvilken grad er de oppgavene som gjennomføres dokumentert og i tråd med loven?

Bruken av begrepene *planlagte og systematiske tiltak* jf. pol § 13 og pof § 2-1 er et tydelig signal om at arbeidet med sikring av personopplysninger skal skje ut i fra en helhetlig vurdering av potensielle sikkerhetstruende hendelser (Schartum 2005:120). Ved en ad hoc og tilfeldig tilnærming til sikringsarbeidet er det lite trolig at resultatet av arbeidet vil være tilfredsstillende. Som jeg kort nevnte i avsnitt 1.4.2 kan kravet om planlagte og systematiske tiltak koples til prinsippet om risikostyring. Dette innebærer at en skal prøve å forutse hendelser som kan være uheldige for sikkerheten. En risikostyrt metode kan slikt sett betegnes som en *proaktiv* tilnærming til sikkerhetsarbeidet (Tranvik 2009:22). Forskriften gir utfyllende regler for gjennomføring av informasjonssikkerhetsarbeidet.

[96] Se pof § 2-3, andre ledd flg.
[97] Se pof §§ 2-4, 2-5 og 2-6.

Bestemmelsene i forskriften viser hvilke tiltak som anses nødvendige for å etablere et tilfredsstillende nivå for beskyttelse av personopplysninger. Det er særlig fire punkter som vil bli tatt opp. Disse er:

- Sikkerhetsmål, -strategi og -organisasjon
- Gjennomføring av risikovurderinger
- Gjennomføring av sikkerhetsrevisjoner
- Arbeid med avvikshåndtering

Det overordnede kravet er at sikkerheten skal være tilfredsstillende jf. pol § 13. Rettslig sett er det dette kravet som vil være bestemmende for omfanget av tiltakene over. Jeg har tidligere diskutert forholdsmessigheten i begrepet *tilfredsstillende* og understreker at vurderingen av hvor omfattende disse tiltakene bør være vil bero på en konkret helhetsvurdering der blant annet virksomhetens størrelse, samt typen og mengden personopplysninger som behandles må tas med i vurderingen (Johansen et. al 2001:130).

## 3.1 Om etablering av sikkerhetsorganisasjon, utarbeidelse av sikkerhetsstrategi og sikkerhetsmål

### 3.1.1 Opprettelse av sikkerhetsorganisasjon

Betegnelsen sikkerhetsorganisasjon er ikke eksplisitt nevnt i lov eller forskrift. Det å etablere en sikkerhetsorganisasjon regnes likevel som et organisatorisk kjerneelement for å lykkes med sikkerhetsarbeidet (Tranvik:2009:90). I forarbeidene til pol nevnes det at både tekniske og organisatoriske tiltak må iverksettes for å møte lovens krav.[98] Opprettelse av en sikkerhetsorganisasjon vil romme flere organisatoriske tiltak.

Pof § 2-7 presiserer at den behandlingsansvarliges øverste ledelse må sette opp tydelige ansvars- og myndighetsforhold. Disse forholdene skal dokumenteres og kan ikke endres uten at det blir godkjent av daglig leder. Dokumentasjonen skal være tilgjengelig og gjøres kjent for alle øvrige ansatte (Johansen et. al 2001:350).

Det er flere faktorer som kan være bestemmende for hvordan en virksomhet utformer sin sikkerhetsorganisasjon. En må forstå det slik at sikkerhetsorganisasjonens utforming vil variere fra virksomhet til virksomhet. I diskusjonen om hva som skal anses for tilfredsstillende må de planlagte og systematiske tiltakene som settes i verk vurderes opp mot sannsynligheten for og konsekvensene av sikkerhetsbrudd jf. pof § 2-1 annet ledd. Eksempelvis vil det i en stor kommune være snakk om flere og mer omfattende behandlinger av personopplysninger enn i en mindre kommune. Det vil også være flere ansatte i en større kommune og således kan en tenke seg at rollene som er beskrevet i oppgavens kapittel 2 vil være fordelt på flere personer i en stor kommune, i motsetning til en mindre kommune hvor flere roller kan være tillagt samme person.

Når loven ikke tilbyr noen detaljert beskrivelse av hvordan en sikkerhetsorganisasjon skal utformes blir det naturlig å se hen til Datatilsynets praksis. I deres veileder fra november 2009 er det vist til et eget dokument kalt ”sikkerhetsorganisasjon”.[99] Dette dokumentet er en god anvisning på hvordan en sikkerhetsorganisasjon kan se ut. Datatilsynet bemerker

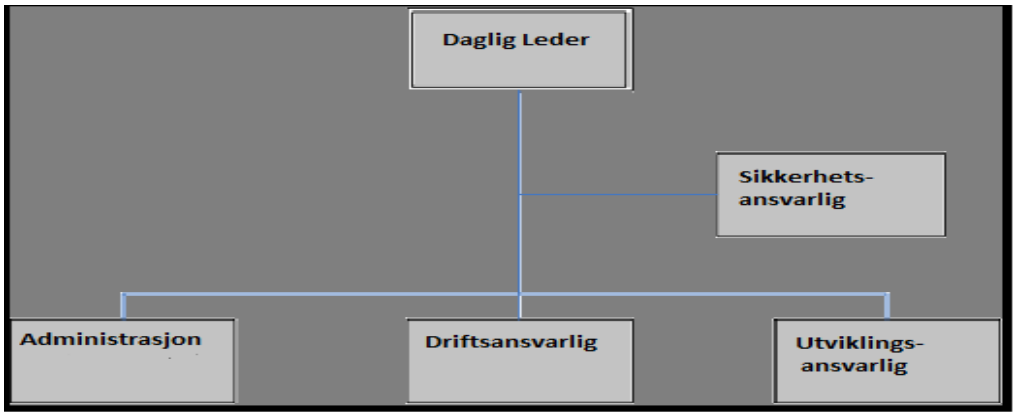
[98] Ot. prp. nr. 92 (1998-99) s. 115
[99] Tilgjengelig på www.datatilsynet.no under veileder og maler. (http://www.datatilsynet.no/upload%5Cdokumenter%5Cinternkontrollfiler%5Cmaler%5C1-12_sikkerhetsorganisasjon.doc)

innledningsvis at; *"eksempelet kan være mer omfattende enn minimumskrav etter personopplysningsloven."*[100]

En sikkerhetsorganisasjon skal angi:

- Rollebeskrivelser
- Myndighet
- Ansvarsområder
- Plikter for virksomhetsleder til driftsansvarlig, for alle de ulike systemene som behandler personopplysninger.

I samme dokument presenteres også en modell av en sikkerhetsorganisasjon:




**Figur 11. Eksempel på hvordan en sikkerhetsorganisasjon kan se ut hentet fra Datatilsynets veiledningsmal "sikkerhetsorganisasjon".**

Initiativet til etablering av sikkerhetsorganisasjon skal komme fra den øverste ledelsen, i modellen er *daglig leder* plassert øverst og dette vil for kommunens vedkommende være rådmannen (se avsnitt 2.5.3 og pof § 2-3). Neste rolle i modellen er *sikkerhetsansvarlig*. Personen med denne rollen vil normalt ha ansvar for ledelsesgjennomganger relatert til sikkerhet, gjennomføring av sikkerhetsrevisjon (se avsnitt 2.9.1 og pof § 2-5) og kontroll med risikovurderinger og avviksbehandling (Johansen et. al 2001:351).

Nederst i modellen finner vi *administrasjon, driftsansvarlig og utviklingsansvarlig.* I følge malen er de sikkerhetsrelaterte oppgavene knyttet til administrasjonen ivaretakelse av fysisk sikkerhet, arkivering og post og ansvar for personell og sikkerhet. Driftsansvarlig vil ha et utøvende ansvar for ivaretakelse av den tekniske sikkerheten knyttet til informasjonssystemene som behandler personopplysninger (Johansen et. al 2001:351). Dette

[100] Ibid.

innebærer oppsett av brannmurer, passordløsninger, sikkerhetskopier etc. Utviklingsansvarlig vil ha ansvar for at nye løsninger som ønskes implementert er i tråd med de krav som sikkerhetsorganisasjonen har satt i forhold til risikovurdering og akseptabel risiko (se avsnitt 3.2). Det at den enkelte kommune ikke har opprettet sikkerhetsorganisasjon i tråd med Datatilsynets modell er som nevnt ikke ensbetydende med at lovens krav ikke er oppfylt. Det viktige er at alt ligger til rette for en tilfredsstillende ivaretakelse av informasjonssikkerheten.

### 3.1.2 Drøftelse av arbeidet med sikkerhetsorganisasjoner i kommunene

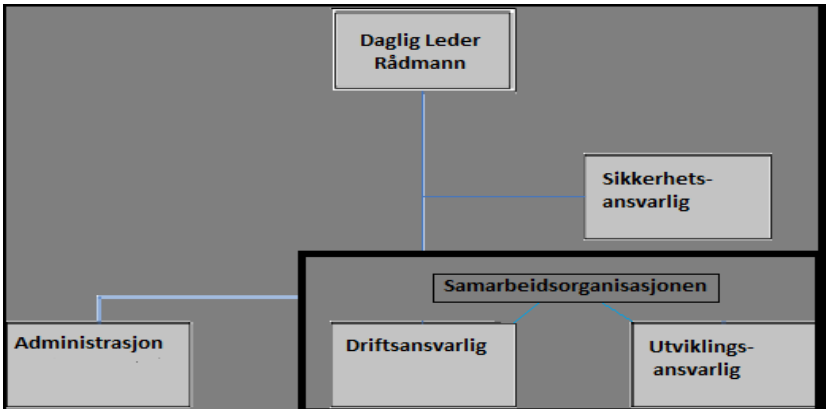
I den felles veilederen for internkontroll og informasjonssikkerhet som skal gjelde for alle kommunene, blir etablering av sikkerhetsorganisasjon tatt opp. I veilederen heter det at "*formålet med sikkerhetsorganisasjonen er å klargjøre ansvars og myndighetsforhold for å sikre at sikkerhetsnivået er tilstrekkelig*." Med utgangspunkt i prinsippet om en ledelsesstyrt tilnærming og Datatilsynets veileder vedrørende etablering av en sikkerhetsorganisasjon, er det kommunenes ledelse, her rådmannen, som skal ta initiativ til etablering av en slik organisasjon.

Ingen av kommunene har dokumentasjon som tilsier at de har opprettet en sikkerhetsorganisasjon lik den som ble vist fra Datatilsynets veileder. På spørsmål om kommunene hadde en komité, arbeidsgruppe eller lignende som jobbet med sikkerhetsrelaterte spørsmål, svarte samtlige nei. Dette kan tyde på at ingen av kommunene har en forankret sikkerhetsorganisasjon. På en annen side har deltakerkommunene, i samråd med samarbeidsorganisasjonen, definert roller som ligner på dem som bør inngå i en sikkerhetsorganisasjon. I SLA- avtalen pkt 2.3 *Roller og ansvar* heter det at " *kunde* (kommunene)[101] *skal sørge for at det oppnevnes systemeier og systemansvarlig for alle fagsystemer som skal benyttes*."[102] Slikt sett kan man si at kommunene har definert og fordelt roller når det gjelder ansvarsområder knyttet til de fagsystemene som er i bruk og som behandler personopplysninger.

Hos samarbeidsorganisasjonen finnes det en oversikt over alle systemeiere og systemansvarlige i de ulike kommunene og oversikten er tilgjengelig på organisasjonens intranett. I den enkelte kommune har de oversikt over systemeiere og systemansvarlige i egen kommune. Kort oppsummert kan en derfor si at alle kommunene formelt sett oppfyller de tre

[101] Min anmerkning
[102] I SLA - avtalens kapittel 3 presenteres også disse rollene og beskrivelsen inneholder klare anvisninger til oppgaver knyttet til behandling av personopplysninger.

første kulepunktene som er angitt i Datatilsynets veileder (avsnitt 3.1.1). Rollebeskrivelser, myndighet og ansvarsområder er definert og dokumentert hos samtlige kommuner. Når det gjelder det siste kulepunktet – angående plikter for de ulike rollene involvert i systemer som behandler personopplysninger, er det noen mangler. Riktignok er pliktene for virksomhetsledere/systemeiere definert og dokumentert, men det finnes ingen driftsansvarlige ute i deltakerkommunene. Alle oppgaver tilknyttet drift er lagt til samarbeidsorganisasjonen og det er dennes ledelse som har pekt ut driftsansvarlig for alle fagsystem som behandler personopplysninger. Pliktene til den driftsansvarlige er fastsatt av samarbeidsorganisasjonen, men inngår i SLA – avtalen slik at alle parter i utgangspunktet er klar over hvilket ansvar som ligger til de som har rollen som driftsansvarlig. I avsnitt 3.1.1 så vi at kommentarene til forskriften særlig påpekte viktigheten av å ha definert ansvar knyttet til driftsledelse og sikkerhetsledelse (Johansen et al. 2001:350). Driftsledelse og driftspersonell er tydelig definert, men er lokalisert i samarbeidsorganisasjonen og ikke i den enkelte kommune.



Figur 12: Etter inngåelse av det interkommunale IKT- samarbeidet har drifts- og utviklingsavdeling blitt sentralisert og flyttet til samarbeidsorganisasjonen sine lokaler.

Etter studier av dokumentasjon og intervjuer med representanter fra samarbeidsorganisasjonen og kommunene er det særlig to funn som gjør at kommunene sin eventuelle sikkerhetsorganisasjon avviker fra den som er skissert av Datatilsynet.

1) For det første er driftsavdelingen og utviklingsavdelingen i praksis skilt ut fra den enkelte kommune og plassert i samarbeidsorganisasjonen. 2) For det andre viser det seg at ingen av kommunene har egen sikkerhetsansvarlig. Dette er to momenter som tydelig synes å ha påvirket organiseringen av informasjonssikkerhetsarbeidet i de fire involverte kommunene.

I avsnitt 1.3.2 viste jeg til prinsippet om ledelsesstyring. Dette blir løftet frem av blant andre Tommy Tranvik[103] og Leif T. Aanensen.[104] Utgangspunktet for dette prinsippet er at arbeidet med sikring av personopplysninger må forankres på ledelsesnivå og at informasjonssikkerhet ikke bare skal være en sak for IKT- ansatte. Det er da ledelsen som skal ta initiativ til

[103] Tommy Tranvik. Personvern og informasjonssikkerhet 2009:22
[104] Leif T. Aanensen. Informasjonssikkerhet – et ledelsesansvar 2008

opprettelse av en sikkerhetsorganisasjon. Oppfatningen blant flere av dem jeg intervjuet i kommunene synes likevel å være at informasjonssikkerhet i hovedsak er en oppgave som løses av samarbeidsorganisasjonen, "kommunenes felles IKT avdeling". Denne holdningen har tilsynelatende hemmende effekt på flere av kommunenes arbeid med informasjonssikkerhet.

Rådmannen i kommune 2 hevdet i et intervju at spørsmål som gjaldt IKT og informasjonssikkerhet ble løst av samarbeidsorganisasjonen og i Kommune 1 ble jeg direkte henvist til samarbeidsorganisasjonen dersom jeg ville vite mer om kommunens arbeid med informasjonssikkerhet.

I kommune 3 stilte det seg litt annerledes enn i kommune 1 og 2. Kommunen hadde besøk av Datatilsynet i 2003. I rapporten fra tilsynet kommer det frem at kommunen i: *alle etater* [må] *utforme dokumentasjon og implementere tiltak etter personopplysningslovens § 13 jf. personopplysningsforskriftens kapittel 2[…].*[105] I tiden etter tilsynet ble det foretatt noe arbeid med informasjonssikkerhet, men den personen som hadde jobbet mest med dette - en IT ansatt, ble senere overført til samarbeidsorganisasjonen og oppmerksomheten rundt informasjonssikkerheten avtok. I intervju med rådmannen i kommune 3 ble det sagt kommunen kanskje ikke hadde hatt nok fokus på personvern den siste tiden, men at den beredskapsansvarlige skulle jobbe mer med informasjonssikkerhet i fremtiden. Og at det felles veiledningsmaterialet utarbeidet av samarbeidsorganisasjonen skulle implementeres.

Hos kommune 4 var bevisstheten omkring eget ansvar noe mer tydelig enn hos de øvrige kommunene. Her hadde en av kommunalsjefene – på instruks fra rådmannen, tatt tak i arbeidet med sikring av personopplysninger og virket veldig bevisst på at det var den enkelte kommune som hadde ansvaret. De hadde enda ikke etablert en sikkerhetsorganisasjon, men var i gang med dette arbeidet. At denne kommunen i mindre grad pekte på samarbeidsorganisasjonen når det kom til ansvar for sikring av personopplysninger forklarte kommunalsjefen med kommunens sene inntreden i samarbeidet. I denne kommunen var de også i prosessen med å utnevne en egen sikkerhetsansvarlig, men ved siste intervju var det enda ikke avklart om det ville bli kommunalsjefen selv eller noen direkte under denne.

I et intervju med en sentral rådgiver i samarbeidsorganisasjonen ble det bekreftet at flere av kommunene la ansvaret for ivaretakelse av informasjonssikkerheten til

[105] Tilsynsrapport fra tilsyn hos kommune 3. 2003.

samarbeidsorganisasjonen og han mente dette var en av årsakene til at sikkerhetsarbeidet i den enkelte kommune fremstod som sporadisk, for ikke å si delvis fraværende.

Alt dette vitner om at holdningen hos mange fortsatt er slik at informasjonssikkerhet er noe for ”folka på IT”. Når IKT- avdelingen og ressursene er sentralisert kan dette tyde på at organiseringen av informasjonssikkerhetsarbeidet i den enkelte kommune blir svekket. Dette bekreftes av rådgiveren i samarbeidsorganisasjonen som trekker frem at veldig mange regner med at samarbeidsorganisasjonen skal ta seg av spørsmål om informasjonssikkerhet.

Opprettelse av en tilfredsstillende sikkerhetsorganisasjon kan være vanskelig når det i praksis ikke er helt klart hvem som ansvar for etableringen og at sikkerhetsorganisasjonen her, kan sies å være delt i to. Etter pol og pof er det den daglige ledelsen - rådmennene i kommunene, som skal ta ansvar for å etablere en sikkerhetsorganisasjon. Samtidig har flere av rådmennene inntrykk av at informasjonssikkerhet er samarbeidsorganisasjonens ansvar og at det er de som skal ta seg av oppgaver som for eksempel etablering av en sikkerhetsorganisasjon.

En mulig løsning på dette problemet kunne vært å etablere sikkerhetsansvarlige i hver enkelt kommune. Dette er også noe samarbeidsorganisasjonen har jobbet for å få til. Dersom en får til dette kan den enkelte kommune ha en person ”på stedet” for å holde overblikk over kommunens arbeid med informasjonssikkerhet.

I intervju med ledelsen i samarbeidsorganisasjonen ble det å ha en sikkerhetsansvarlig i hver kommune løftet frem som et sterkt ønske. Man antok at et slikt tiltak ville gjøre det lettere å koordinere sikkerhetsarbeidet og implementere den felles veilederen fullt og helt. En annen årsak til at den enkelte kommune bør få på plass en sikkerhetsansvarlig er at for mye ansvaret for ivaretakelse av sikkerheten tilsynelatende blir lagt til samarbeidsorganisasjonen. En sikkerhetsansvarlig kunne også ha koordinert kommunenes opprettelse av en sikkerhetsorganisasjon.

Det er viktig å understreke at det ingen steder i lov eller forskrift stilles krav til at en virksomhet skal ha en egen sikkerhetsansvarlig. Selv om en slik rolle anbefales. I den felles veilederen er sikkerhetsansvarliges oppgave skissert å være:

- Godkjenne større endringer av infrastrukturen og programvaren.
- Ajourholde oversikt over kommunenes informasjonssystemer med samarbeidsorganisasjonen, systemeiere og systemansvarlige

- Motta og følge opp gjennomførte sikkerhetsrevisjoner fra systemeiere
- Årlig å arrangere sikkerhetsforum for systemeiere, systemansvarlige og driftsansvarlige
- Årlig å gjennomføre og følge opp ledelsens gjennomgang i forhold til fastlagt prosedyre.

Per i dag er det altså ingen av kommunene som har utnevnt en person til en slik rolle, selv om kommune 2 og 4 meget snart vil ha en slik person på plass. Det vil ikke være aktuelt for noen av kommunene å ha en person med sikkerhetsleder som full stilling. Det er mer sannsynlig at stillingsbrøken vil ligge på mellom 20 og 30 prosent. Dette blir begrunnet ut i fra knappe ressurser og høyt press på arbeidsoppgaver. Med det sagt, så kan man se ut i fra de angitte oppgavene til en sikkerhetsansvarlig (over) at en person med denne stillingen fort kunne blitt det koordinerende ledd som mangler mellom kommunene og samarbeidsorganisasjonen.

### 3.1.3 Sikkerhetsmål og strategier

Pof § 2 -3, første ledd sier at det er den daglige ledelsen av den behandlingsansvarliges virksomhet som skal påse at bestemmelsene i hele kapittel 2 følges. Dette vil for kommunene her være deres rådmenn. Videre heter det at formål med behandlingene og overordnede føringer for bruk av IKT skal inngå i sikkerhetsmål. I følge Datatilsynet er det sikkerhetsmålene som skal danne grunnlaget for kommunens totale sikkerhetsstrategi.[106]

Pof § 2-3, tredje ledd pålegger den enkelte rådmann ansvaret for at det gjøres valg og prioriteringer for sikkerhetsarbeidet. Dokumentasjonen knyttet til sikkerhetsorganisasjonen skal også inngå i sikkerhetsstrategien (se avsnitt 3.1.1). Sikkerhetsstrategien skal inneholde en redegjørelse av tekniske og organisatoriske tiltak som er gjort i forhold til sikkerhetsarbeidet. Datatilsynet legger vekt på at disse skal være utformet på en slik måte at de øvrige ansatte forstår hva ledelsen har bestemt.[107]

Pof § 2-3, fjerde og femte ledd slår fast at informasjonssystemene skal gjennomgås jevnlig for å sikre at sikkerhetsstrategien ivaretar lovens krav om tilfredsstillende sikkerhet. Videre skal de vurderingene som gjøres ved den jevnlige gjennomgangen legge grunnlag for eventuell endring av sikkerhetsstrategi og sikkerhetsmål.

[106] En veiledning om internkontroll og informasjonssikkerhet. Datatilsynet 2009:23
[107] En veiledning om internkontroll og informasjonssikkerhet. Datatilsynet 2009:23

I følge IKT- samarbeidets felles veileder for internkontroll og informasjonssikkerhet pkt 2.1 om sikkerhetsmål heter det at ” kommunen skal etablere den grad av informasjonssikkerhet som er påkrevet i henhold til personopplysningsloven”. Dette er også alt som står. Til en veileder å være, er ikke denne formuleringen mye til hjelp. Sikkerhetsmål skal blant annet omfatte; til hva og hvordan informasjonsteknologi benyttes i den enkelte virksomhet (Johansen et al. 348: 2001). Datatilsynet forklarer i sin veileder at sikkerhetsmålene bør være relativt konkrete.[108]

Ingen av kommunene jeg snakket med hadde utformet dokumentasjon vedrørende sikkerhetsmål. I utgangspunktet ligger ansvaret for å etablere sikkerhetsmål til deltakerkommunenes rådmenn, men en kan tenke seg at denne oppgaven blir delegert til virksomhetsleder/systemeier og at de fastsetter sikkerhetsmål innenfor eget virksomhetsområde. Når hvert informasjonssystem skal gjennomgås, er nok den enkelte systemeier bedre skikket til dette enn rådmannen. Men rådmannen har ansvaret for å påse at disse prosessene blir gjennomført. Ingen av kommunene jeg snakket med kunne vise til at sikkerhetsmål var dokumentert separat for den enkelte kommunes virksomheter.

I og med at fastsettelse av sikkerhetsmål først og fremst skal handle om å stadfeste formål med behandling av personopplysninger og til hva og hvordan informasjonsteknologi skal brukes jf. pof § 2-3 annet ledd, kan det tenkes at sikkerhetsmål er noe som bør diskuteres mellom deltakerkommunene og samarbeidsorganisasjonen. Mer spesifikt den enkelte systemeier og den enkelte driftsansvarlige. Det er samarbeidsorganisasjonen som besitter den tekniske kompetansen og det er de som drifter de fleste fagsystemene på vegne av kommunene. Det vil derfor være de som er mest skikket til å angi til hva og særlig hvordan informasjonsteknologi skal brukes, mens den enkelte kommune som behandlingsansvarlig bestemmer formålene med deres behandlinger av personopplysninger.

Når det gjelder utarbeidelse av sikkerhetsstrategi hos kommunene, kan en si det slik at innholdet til en strategi finnes, men at det er ikke dokumentert. Pof § 2 -3, tredje ledd sier at sikkerhetsstrategien skal inneholde organisatoriske og tekniske tiltak som er gjort i forhold til gjennomføring av sikkerhetsarbeidet. Ved gjennomgangen av roller i kapittel 2, så vi at alle kommunene og samarbeidet hadde avklart ansvars- og myndighetsforhold og at ansvarsforhold var regulert. Dette er en type av organisatoriske tiltak som bør inngå i en

[108] En veiledning om internkontroll og informasjonssikkerhet. Datatilsynet 2009:22

sikkerhetsstrategi. Andre organisatoriske tiltak er oppnevnelse av sikkerhetsansvarlig og etablering av sikkerhetsorganisasjon. Sistnevnte har vi sett at kun i begrenset grad er gjennomført hos deltakerkommunene.

På samme måte som ved utarbeidelse av sikkerhetsmål, kan det tenkes at utarbeidelse av sikkerhetsstrategi bør skje i samråd med samarbeidsorganisasjonen. Begrunnelsen for dette er at også her er samarbeidsorganisasjonen som besitter den tekniske kompetanse, og at det er de som drifter fagsystemene som behandler personopplysninger på vegne av kommunene. Det vil derfor være naturlig at noen i samarbeidsorganisasjonen er med på å fastsette hvilke tekniske tiltak som skal inn i sikkerhetsstrategien. Eksempler på slike tiltak kan for eksempel være vurderinger knyttet til tilgangskontroll, kryptering og soneinndeling.[109]

## 3.2 Om akseptabel risiko og risikovurderinger

Risikovurderinger er kjernen i en risikostyrt tilnærming til informasjonssikkerhet. I foregående avsnitt så vi at ansvar for utarbeidelse av sikkerhetsmål og sikkerhetsstrategi ligger hos virksomhetens ledelse. Det samme er tilfellet hva gjelder risikovurderinger.

Fra forskriftsmyndighetenes side har man helt bevisst valgt å kalle det for risiko*vurdering* i stedet for risiko*analyse*, som kanskje er mer vanlig. Dette er gjort for å klargjøre at arbeidet med å avdekke risiko ikke skal være mer omfattende enn det som er nødvendig (Johansen et al. 2001:349). Denne vurderingen kan ses i sammenheng med pof § 2-1 sitt krav om en forholdsmessig tilnærming til sikkerhetsarbeidet og at en virksomhets arbeid med sikring av personopplysninger skal stå i forhold til dens størrelse og omfanget av personopplysninger som behandles, samt opplysningenes grad av sensitivitet.

Oppgaver knyttet til gjennomføring av risikovurderinger kan delegeres. Det er kanskje også naturlig at den med det daglige ansvaret koordinerer arbeidet med risikovurderinger innenfor sitt virksomhetsområde fordi denne personen vil være nærmere ”der det skjer” enn den øverste ledelsen. En kan også anta at den som har det daglige ansvaret innenfor et virksomhetsområde har spisskompetanse til å vurdere sannsynlighet for brudd og konsekvenser av brudd innenfor et konkret virksomhetsområde i motsetning til rådmannen. Det øverste ansvaret vil uansett ligge hos kommunenes rådmenn.

[109] Det er vanlig å dele inn en virksomhets område inn i ulike (gjerne fysisk adskilte) sikkerhetssoner. Eksempelvis kan en gradere sikkerhetssoner fra 1-4. Sikkerhetssone 1 betegner områder med tilnærmet fri ferdsel og som ikke rommer teknisk kritiske ressurser. Sikkerhetssone 4 betegner data-/ serverrom som er viktige for virksomheten å sikre (Daler et al. 2006:218 flg.).

Det er pof § 2-4 som regulerer risikovurderinger. Bestemmelsens første ledd pålegger den aktuelle virksomhet å føre en oversikt over de personopplysninger som behandles i virksomheten. Virksomheten skal selv fastlegge kriterier for hva som skal anses for akseptabel risiko etter § 2-4 første ledd siste setning. § 2-4 annet ledd pålegger videre virksomheten at en risikovurdering skal gjennomføres for å kartlegge sannsynligheten for og konsekvensene av sikkerhetsbrudd.

Dette betyr at kommunene og de ulike virksomhetene innefor kommunene selv må finne ut hva som er god nok sikkerhet for dem ved å gjøre en vurdering av hva som kan anses som tilfredsstillende sikkerhet jf. pol § 13. Gjennomføring av risikovurderinger krever helt klart både juridisk og teknisk kompetanse hos virksomheten, men Datatilsynet kan imidlertid bidra på to måter. 1) i form av pålegg og gjennom deres rolle som veiledende organ. I pof er det tatt inn en bestemmelse som gir Datatilsynet adgang til å bestemme hva som skal anses for akseptabel risiko for en virksomhet jf pof § 2-2. 2)Datatilsynet har også en veiledningsfunksjon og som ledd i dette har de utformet mange veiledere og maler, blant annet en veileder om hvordan risikovurderinger kan gjennomføres[110].

Kommer det frem av risikovurderingen at risikoen for brudd på sikkerheten er større en det som er angitt som akseptabelt risikonivå, må tiltak settes i verk for å få risikoen ned på akseptabelt nivå. I Datatilsynets veileder heter det at "akseptabelt risikonivå skal fastlegges for alle sikkerhetsbehov, herunder konfidensialitet, tilgjengelighet og integritet.[111] Risikovurderingen skal dokumenteres jf. fjerde ledd. Det er viktig å forstå at risikovurderingen også skal være "løpende." Pof § 2-4 andre ledd sier blant annet det skal foretas nye risikovurderinger dersom det blir gjort endringer av betydning for sikkerheten. Eksempler på hva som kan kreve ny risikovurdering er bl.a.:

- Endringer i trusselbildet
- Endring i klassifisering av opplysninger
- Organisasjonsendringer

### 3.2.1 Drøftelse av akseptabel risiko og risikovurderinger i kommunene

I følge IKT- samarbeidets felles veileder for internkontroll og informasjonssikkerhet er oppgaven med å gjennomføre risikovurderinger lagt til den enkelte

[110] Datatilsynet – "Risikovurdering av informasjonssystemer"
[111] Datatilsynets veileder om internkontroll og informasjonssikkerhet. 2009:25

systemeier/virksomhetsleder. Dette må sies å være et godt valg, fordi en systemeier/virksomhetsleder antageligvis vil ha mer kunnskap om behandlingene som skjer innenfor sin virksomhet enn det rådmannen ville ha hatt. I veilederen heter det at "*systemeier skal gjennomføre risikovurdering ved større endringer med betydning for sikkerheten*." Etter samtaler med representanter fra den enkelte kommune kommer det likevel frem at det pr i dag ikke foreligger rutiner for å gjennomføre slike risikovurderinger, følgelig blir disse ikke utført.

I kommune 1 snakket jeg med en virksomhetsleder. Han mente at de ikke hadde noen konkrete rutiner for risikovurderinger, men at sikkerheten var god. Dette begrunnet han med at de hadde god kontakt med samarbeidsorganisasjonen og visste at de ivaretok den tekniske sikkerheten på en god måte. Samtidig hadde han en systemansvarlig under seg som ivaretok de daglige oppgavene knyttet til sikkerhet som for eksempel tildeling av rettigheter og passord. I 2007 hadde en avdeling innefor hans virksomhet hatt besøk av Datatilsynet. Fra deres rapport kom det frem at avdelingen "*har etablert flere sporadiske rutiner som retter seg mot praktiske tiltak for behandling og sikring av personopplysninger."*[112] Rapporten viste videre at disse sporadiske tiltakene langt i fra var gode nok. Virksomhetslederen jeg snakket med sa at representanter fra samarbeidsorganisasjonen hadde jobbet for å rette opp avvikene og at Datatilsynet hadde fått tilsendt dokumentasjon som viste at avvik knyttet til informasjonssikkerhet - herunder risikovurderinger, og internkontroll var ordnet. Likevel opplyste han at de i per i dag ikke hadde fulgt opp og brukt denne dokumentasjonen i særlig grad.

I kommune 2 snakket jeg med rådmannen og en systemansvarlig vedrørende risikovurderinger. Rådmannen tvilte på at kommunen hadde et godt regime for gjennomføring av risikovurderinger. Jeg snakket også med en systemansvarlig, som hadde fått delegert en del oppgaver fra systemeier. Hun forklarte at de hadde en god kultur for sikkerhet særlig med tanke på taushetsplikt, passordløsninger og tilgangskontroll. Hun viste også til forvaltningslovens bestemmelser om taushetsplikt som gjaldt for alle ansatte. Når det kom til risikovurderinger, var disse mer eller mindre fraværende. På spørsmål om dette var noe de kom til å jobbe for å få på plass var svaret at hun ønsket å si ja, men tvilte på at det ble noen særlig endringer dersom det ikke kom pålegg direkte fra sjefen. Dette ble begrunnet i

[112] Tilsynsrapport fra besøk hos kommune 1. 2007.

knapphet på ressurser og stor arbeidsmengde. Hun mente likevel at det var en god kultur for ivaretakelse av brukeres personlige opplysninger i virksomheten.

I kommune 3 snakket jeg med rådmannen og en beredskapskoordinator om gjennomføring av risikovurderinger. Rådmannen presiserte tidlig i intervjuet at han ikke var særlig godt kjent med reglementet og detaljer omkring informasjonssikkerhetsarbeid. Han var usikker på regimet for gjennomføring av risikovurderinger i kommunen, men antok at det ble gjort. Jeg ble henvist til kommunens beredskapskoordinator for spørsmål vedrørende informasjonssikkerhet og spørsmål av teknisk karakter. Beredskapskoordinatoren fortalte at det ble gjennomført risikoanalyser i sammenhang med utarbeidelse og revisjon av kommunens beredskapsplan. Her inngikk også et kapittel om IKT.

De analysene som er gjort omkring denne kommunens bruk av IKT i bredskapsplanen kan nok bare telle marginalt i forhold til arbeid med sikring av personopplysninger. Beredskapsplanen inneholder risikoanalyser om IKT knyttet til backupløsninger ved bortfall av strøm eller konsekvensvurderinger i forhold til naturkatastrofer etc. Riktignok er dette viktige momenter, men det er ikke risikovurderinger gjort i det øyemed å sikre personopplysninger. Den beredskapsansvarlige mente at risikovurderinger knyttet til informasjonssikkerhet og personvern var en oppgave som lå til samarbeidsorganisasjonen.

I kommune 4 snakket jeg med kommunalsjefen som blant annet har ansvaret for kommunens egen avdeling for IKT og beredskap. Her ble jeg fortalt at det til nå ikke hadde eksistert noen felles strategi for gjennomføring av risikovurderinger og i den grad noe var blitt gjennomført så var det i beste fall hos få avdelinger og av rimelig sporadisk karakter. Dette var imidlertid i ferd med å endres. Rådmannen i kommunen hadde selv tatt opp viktigheten av internkontroll og informasjonssikkerhet og IKT- avdelingen jobbet nå mot sertifisering hos Veritas og for at rutiner for internkontroll og informasjonssikkerhet skulle skjerpes. Her ble gjennomføring av risikovurderinger særlig løftet frem. I motsetning til kommune 1 og 3 synes kommune 4 å ha tatt et klart grep om sitt eget ansvar. Selv om de ikke er i mål med etablering og gjennomføring av risikovurderinger, er de tydelige på at det er deres eget ansvar og arbeidet er igangsatt.

Oppgavene til de ulike rollene er dokumentert i SLA – avtalen og i den felles veilederen. I praksis synes oppgavene å mangle forankring i kommunene og samarbeidsorganisasjonen. Med dette mener jeg at flere arbeidsoppgaver vedrørende informasjonssikkerhet er knyttet til

bestemte roller på papiret, men at det i praksis ikke er helt tydelig hvem som skal gjøre hva. Dette blir særlig tydelig når det kommer til risikovurderinger. Noen av personene jeg har snakket med legger ansvaret til samarbeidsorganisasjonen og noen tar initiativ selv. Samarbeidsorganisasjonen på sin side gir uttrykk for at kommunene må gjøre mer selv. En faktor som kan være utslagsgivende her er konsentrasjonen og sentraliseringen av IKT-kompetansen. Drift og utvikling er sentralisert og flyttet til samarbeidsorganisasjonens lokaler og det finnes ingen sikkerhetsansvarlig i den enkelte kommune. Dette kan være medvirkende til at den enkelte kommunes arbeid med å skape en felles strategi for gjennomføring av risikovurderinger ikke lykkes. Det er også bemerkelsesverdig at gjennomføring av risikovurderinger er dokumentert som systemeiers oppgave, mens man fra kommunene 1,2 og 3 sin side raskt legger denne oppgaven til samarbeidsorganisasjonen. Her ser en tydelig at dokumentasjonen ikke samsvarer med praksis.

Likevel er det samarbeidsorganisasjonen som i hovedsak drifter fagsystemene for deltakerkommunene. De tekniske vurderingene i forhold til gjennomføring av risikovurderinger er det derfor de som har kompetanse til å foreta. Slikt sett ville det kanskje vært mer hensiktsmessig å samarbeide om gjennomføring av risikovurderinger. Antageligvis er den enkelte kommune selv best skikket til å vurdere risiko i forhold til personellsikkerhet, intern dokumentasjonssikkerhet og til en hvis grad fysisk sikkerhet. Samarbeidsorganisasjonen – med sin sterke IKT- kompetanse, er best skikket til å vurdere kommunenes sikkerhetsbehov med hensyn til systemteknisk sikkerhet og driftsrutiner.

Et siste moment som kan være med å utsette iverksetting av risikovurderinger i den enkelte kommune er kvaliteten på veiledningsmaterialet, herunder de felles retningslinjene for internkontroll og informasjonssikkerhet. Jeg har tidligere vist til den uklare rollen samarbeidsorganisasjonen spiller i forhold til informasjonssikkerhetsarbeidet. Men de har helt klart tatt på seg ansvaret med å utarbeide den felles veilederen og det sitter også personell med god kunnskap om informasjonssikkerhet i organisasjonen. Dersom det er slik at deltakerkommunene skal bruke denne veilederen som rettesnor for sitt informasjonssikkerhetsarbeid, bør veilederen være godt utformet. Det er den også på mange områder, men når det kommer til gjennomføring av risikovurderinger har veilederen én stor mangel; den tar ikke opp spørsmålet om etablering av akseptabelt risikonivå.[113]

[113] Kommunenes felles veileder for internkontroll og informasjonssikkerhet.

Risikovurderinger skal gjøres ut i fra fastlagte kriterier for hva som anses å være et akseptabelt risikonivå. Når risikonivået overstiger det nivået som er definert som akseptabelt skal tiltak iverksettes. Den felles veilederen sier ingenting om etablering av akseptabelt risikonivå. Og da blir spørsmålet hvordan den enkelte kommune skal gjennomføre gode risikovurderinger når de på forhånd ikke har definert et akseptabelt nivå?

På dette punktet bør veilederen styrkes og risikonivåene innenfor de ulike virksomhetene bør kartlegges slik at de som skal gjennomføre risikovurderinger har noe å vurdere risiko opp i mot.

## 3.3 Sikkerhetsrevisjon og avvik

Pof § 2-5 slår fast at det jevnlig skal foretas sikkerhetsrevisjon. Denne bestemmelsen gir uttrykk for at den behandlingsansvarlige regelmessig skal etterprøve sitt arbeid med sikkerhet og vurdere om de tiltak som er iverksatt for å nå tilfredsstillende sikkerhet fungerer som de skal (Johansen et al. 2001:350). En forutsetning for revisjonsprosessen er derfor at den enkelte kommune allerede har gjort et godt arbeid med sikkerhetsmål, strategi og risikovurderinger. I kommentarene til forskriften karakteriseres sikkerhetsrevisjoner som et viktig grunnlag for stadig utbedring av en virksomhets sikkerhetsarbeid (ibid.). Sikkerhetsrevisjon blir ikke eksplisitt nevnt i forarbeidene, men det slås fast at det "*bør lages rutiner for hvordan* [sikkerhets-] *tiltakene skal vurderes.*"[114] Ved regulering av sikkerhetsrevisjon i pof § 2-5, må man kunne si at forskriften gjennomfører oppfordringen fra forarbeidene. Med sikkerhetstiltak må man i denne sammenheng for eksempel forstå organisatoriske, tekniske, fysiske og personelle tiltak som kan ha betydning for sikkerheten.

I likhet med andre oppgaver knyttet til organisering og gjennomføring av sikkerhetsarbeidet er det viktig at ansvaret for sikkerhetsrevisjon formelt blir tildelt noen i den behandlingsansvarliges virksomhet. Det mest nærliggende, sett ut i fra forskriften, er å tillegge denne oppgaven til en sikkerhetsrevisor (avsnitt 2.7). Vi har sett at det i mindre virksomheter kan være for mye forlangt at sikkerhetsrevisor skal utgjøre en egen stilling. Uansett er det nok tilrådelig å ha en person som har revisjonsoppgaver knyttet til sin stilling.

Etter pof § 2-5, andre ledd skal sikkerhetsrevisjonen blant annet vurdere organiseringen av sikkerhetsarbeidet og sikkerhetstiltak.

[114] Ot.prp. nr. 92 (1998-99) s.115.

Bestemmelsens siste ledd sier at dersom sikkerhetsrevisjon avdekker brudd på sikkerheten, så skal disse bruddene behandles som avvik.

Avvikshåndtering reguleres i pof § 2-6. Med avvik forstår vi ”*bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.”* Man kan i utgangspunktet tenke seg at dette handler mest om sikkerhetsbrudd av teknisk eller personell karakter. Men håndtering av avvik stiller også krav til organisatoriske tiltak. I dette ligger det at avvik skal dokumenteres og at man skal arbeide mot å oppnå normal tilstand og hindre gjentagelse. Her ligger det implisitt at noen må ha ansvar for avvikshåndteringen og at det må foreligge rutiner for hvordan det skal skje.

### 3.3.1 Drøftelse av sikkerhetsrevisjon og avvik i kommunene

I avsnitt 3.1.1 og 3.2.1 har vi sett at sikkerhetsmål, strategi, etablering av akseptabelt risikonivå og gjennomføring av risikovurderinger er mangelvare hos kommunene. Med utgangspunkt i disse manglene kan man si at det heller ikke foreligger noe særlig godt grunnlag for gjennomføring av revisjon.

I følge den felles veilederen for internkontroll og informasjonssikkerhet skal systemeier/virksomhetsleder gjennomføre prosedyre for sikkerhetsrevisjon.

I kommune 1 snakket jeg med en virksomhetsleder om dette. Datatilsynet har vært på besøk hos en avdeling i hans virksomhet. Det ble påpekt en del feil og han fortalte at de etter kontrollen hadde ”tatt en ny runde” på tildeling av roller og ansvar. Dette kan betegnes som revisjon. I denne forbindelse påpekte han også at en representant fra samarbeidsorganisasjonen hadde vært til stede ved kontrollen og at det var han som hadde ordnet opp i de fleste av manglene. Når det gjelder avviksrapportering påpekte systemeieren at den systemansvarlige som var på stedet tok seg av små problemer knyttet til tilganger og passord. Videre ble det forklart at det var samarbeidsorganisasjonen som leverte linje og servere og at det var de som måtte rette opp eventuelle feil. Ellers hadde de ikke et fast regime for innrapportering av avvik knyttet til informasjonssikkerhet og sikring av personopplysninger.

I kommune 2 snakket jeg med beredskapskoordinator om dette, han gjentok fra vår samtale om risikovurderinger at han hadde som oppgave å revidere kommunens beredskapsplan og at det inn under denne lå noen punkter om IKT, men de var ikke i direkte grad knyttet til sikring av personopplysninger. Det var noe samarbeidsorganisasjonen skulle ta seg av.

I kommune 3 fortalte en systemansvarlig at de ikke hadde noen spesielle rutiner for sikkerhetsrevisjon. I og med at gjennomføring av risikovurderinger heller ikke var på plass i denne kommunen, så er kanskje mangelen på rutiner for revisjon ikke helt uventet.

I kommune 4 var de i ferd med å etablere et omfattende system for internkontroll og informasjonssikkerhet. Gjennomgang skulle forekomme hvert fjerde kvartal og gjennomgangen ville innebefatte revisjon av sikkerhetsnivået i kommunen. Arbeidet var i gang, men revisjon hadde enda ikke blitt gjennomført sist jeg var i kontakt med dem.

Når det gjelder avviksrapportering fant jeg at dette var mer utbredt hos kommunene og hos samarbeidet. Avvik avhengig av dets karakter ble enten rapportert til driftsavdelingen i samarbeidsorganisasjonen eller til systemeier/-ansvarlig i den enkelte kommune. Avvik vedrørende bortfall av internett, intranett og eller nedetid i fagsystem, ble tatt opp med driftspersonalet i samarbeidet, mens avvik vedrørende passord og oppdateringer ble tatt internt i kommunen.

Til tross for at avvik blir rapportert inn var det ingen av kommunene som kunne vise til dokumentasjon over hva man målte avvik ut i fra. Systemansvarlig i kommune 3 fortalte at folk som regel forsto dersom noe var galt fordi de som følge av avviket ble hindret i sitt arbeid og var derfor raske til å rapportere dette. Avviksmeldinger kunne komme over telefon, på e-post eller muntlig. Samme fremgangsmåte så ut til å være valgt i kommune 2. På spørsmål om hva de målte avvik ut i fra var svaret at folk flest skjønte hva som var avvik. Dersom ansatte eventuelt var usikre på hva som var et avvik meldte de det inn, og dermed var det opp til systemeier/systemansvarlig eller driftsansvarlig i samarbeidsorganisasjonen å vurdere om det var et avvik eller ikke.

## 3.4 Samlet vurdering av gjennomførende tiltak for organisering av informasjonssikkerhetsarbeid i kommunene.

I kapittel to så vi at de ulike rollene knyttet til sikkerhetsarbeidet var relativt godt dokumentert i alle kommunene og i samarbeidsorganisasjonen. Vi så likevel at roller som sikkerhetsansvarlig og sikkerhetsrevisor ikke var etablert i kommunene. Etter gjennomgangen av rettslige krav knyttet til gjennomføring av informasjonssikkerhetsarbeidet i dette kapittelet har vi sett at rollene som er dokumentert kun i varierende grad gjennomfører sine oppgaver i praksis.

Rådmennene har det øverste ansvaret for iverksetting av tiltak som etablering av sikkerhetsorganisasjon, utforming av sikkerhetsmål og strategier, samt å påse at nivå for akseptabelt risikonivå og gjennomføring av risikovurderinger finner sted.

Den enkelte systemeier har fått ansvar for å gjennomføre risikovurderinger og sikkerhetsrevisjon innenfor sitt virksomhetsområde. Ingen av kommunene har et felles regime for gjennomføring av risikovurderinger og i den grad gjennomføring av risikovurderinger skjer, er det kun sporadisk.

Vi har sett at to av kommunene har hatt besøk av Datatilsynet. En kommune i 2003 og en annen i 2007. Kontrollbesøkene ser ut til å ha hatt en virkning på kommunenes fokus på informasjonssikkerhet, men virkningen ikke har vart så lenge. Dette stemmer også overens med funnene Tranvik gjorde i sine studier av informasjonssikkerhet i norske kommuner. Han fant at fokus på informasjonssikkerhet – særlig fra ledelsens side, fikk en opptur etter besøk fra tilsynet, men interessen falmet etter hvert (Tranvik 2009:53).

Et moment som synes å være gjennomgående hos kommunene er at samarbeidsorganisasjonen etter deres oppfatning er ansvarlige for ivaretakelse av informasjonssikkerheten. Jeg har tidligere slått fast at hver enkelt kommune er behandlingsansvarlig for de personopplysninger de behandler og dermed er det den enkelte kommune som er ansvarlig for at reglene i pol § 13 og pof kapittel 2 etterleves. Til tross for dette synes mange å mene at det er samarbeidsorganisasjonen som har ansvar de ulike oppgavene knyttet til ivaretakelse av regelverket.

Det at det er uklart hvem som skal gjøre hva, virker naturligvis hemmende på sikkerhetsarbeidet. Forskriften peker på flere tiltak som bør være på plass for at sikkerheten skal anses som tilstrekkelig. Problemet er at mange av disse tiltakene henger tett sammen.

Dette betyr for eksempel at når det ikke er fastlagt noe akseptabelt risikonivå, så er det vanskelig å gjennomføre gode risikovurderinger. Har man ikke gjennomført risikovurderinger, så mangler man igjen grunnlag for å gjennomføre sikkerhetsrevisjoner.

Denne typen ”følgefeil” er synlig hos alle kommunene. Den felles veilederen for internkontroll og informasjonssikkerhet er også mangelfull. Den sier ingenting om etablering av akseptabelt risikonivå og er heller ikke særlig spesifikk når den tar for seg sikkerhetsmål og strategier. Det kan kanskje også være aktuelt å be om assistanse fra for eksempel Datatilsynet om hvordan en kan utforme en veileder som er mer tilpasset interkommunale IKT- samarbeid.

For å bedre situasjonen når det kommer til de gjennomførende tiltakene bør den enkelte kommune (ledelsen inkludert) og den enkelte ansvarlige innenfor de ulike virksomhetsområdene i større grad få klargjort sitt ansvar. Veilederen bør tas i bruk og forbedres. Samarbeidsorganisasjonen bør på sin side i større grad bidra med assistanse når det gjelder vurdering av tekniske tiltak.

Inngåelsen av det interkommunale IKT- samarbeidet har ført til at den tekniske kompetansen har blitt sentralisert. I teorien kan en derfor si at en eventuell sikkerhetsorganisasjon vil være delt i to og at det ikke er noen igjen i kommunene med kompetanse til å vurdere tekniske tiltak vedrørende informasjonssikkerhet. En mulig løsning på denne utfordringen er at systemeiere og/eller systemansvarlige innefor de ulike virksomhetsområdene møter med teknisk personell som har ansvar for fagsystemene fra samarbeidsorganisasjonens side. Sammen kan de vurdere risiko knyttet til de aktuelle fagsystem.

# 4 Om IKT- samarbeidets innvirkning på kommunenes informasjonssikkerhetsarbeid.

I de foregående kappitlene har fokuset vært rettet mot hvordan ansvar og myndighet er fordelt mellom kommunene og samarbeidsorganisasjonen og hvordan de lovpålagte oppgavene for gjennomføring av informasjonssikkerhetsarbeid er løst i deltakerkommunene. Vi har sett at alle kommunene selv har rettslig ansvar som behandlingsansvarlig for de personopplysningene som behandles i kommunen og at samarbeidsorganisasjonen ikke kan karakteriseres som databehandler. På en annen side har jeg vist at samarbeidsorganisasjonen har tatt på seg flere roller knyttet til informasjonssikkerhet. Noe ansvar har tilfalt samarbeidsorganisasjonen naturlig i og med at alle driftsresurser har blitt samlet i felles lokaler. Andre roller har de fått fordi flere har inntrykk av at informasjonssikkerhet er noe for IKT- ansatte. Fordi samarbeidsorganisasjonen betraktes som en felles IKT- avdeling anser flere fra kommunene det som naturlig at det er samarbeidsorganisasjonen som skal ta seg av de oppgavene som er knyttet til informasjonssikkerhet. Det er liten tvil om at etableringen av det interkommunale IKT- samarbeidet har påvirket den enkelte kommunes arbeid med informasjonssikkerhet. I følgende kapittel forsøker jeg å samle de funnene jeg har gjort knyttet til ansvar og roller (kapittel 2) samt gjennomgangen av lovpålagte oppgaver knyttet til informasjonssikkerhetsarbeidet (kapittel 3) for å svare på følgende spørsmål:

3. I hvilken grad den interkommunale samarbeidsorganisasjonen påvirker informasjonssikkerhetsarbeidet i den enkelte kommune.

    a. Om samarbeidet har endret kommunenes arbeid med informasjonssikkerhet på noen måte, eller om alt er som før?
    b. Om inngåelsen av interkommunalt IKT – samarbeid styrker den enkelte kommunes ivaretakelse av informasjonssikkerhet knyttet til behandling av personopplysninger?

## 4.1 Konsentrasjon av IKT- kompetanse.

En av de faktorene som ser ut til å ha gjort størst utslag på deltakerkommunenes arbeid med informasjonssikkerhet er sentraliseringen av IKT – kompetansen. Med sentralisering mener jeg her at alle personer med formell IKT- kompetanse fra deltakerkommunene er samlet i felles lokaler. Dette er med unntak av kommune 4 som enda ikke har overført noe personell. Det er kommune 1 som har arbeidsgiveransvar for alle som er ansatt i samarbeidsorganisasjonen. Som vi så i avsnitt 1.3.2 er tradisjonelle målsetninger for inngåelse av interkommunalt samarbeid ønsket om kompetanseheving og (kostnads-) effektivitet [115]. Disse målsetningene samsvarer med de målene deltakerkommunene hadde før inngåelse av samarbeidet. Prosjektrapporten som ble utarbeidet forut for inngåelse av samarbeidet viser at det å samle IKT- kompetansen i et felles driftsmiljø var en måte å oppnå disse målene på. Som vist i avsnitt 1.3.3 bidro kommune 2 og 3 med henholdsvis 1 og 2 personer, mens kommune 4 enda ikke har flyttet noen over. Slikt sett kan man si at bidragene fra kommunene utenom kommune 1 var relativt beskjedne og utgjør totalt bare tre personer. Dette begrunnes i at kommune 2 og 3 er små og hadde lite IKT- personell. Mangelen på IKT- personell og midler til å forsterke disse kommunenes IKT- avdelinger var en direkte årsak til at kommune 2 og 3 ønsket å bli med på samarbeidet (se avsnitt 1.3.3).

Kommune 4 ble ikke medlem av samarbeidet før 01.01.10 og det er enda ikke klart om de skal bidra med personell. Daglig leder i samarbeidsorganisasjonen fortalte i et intervju at de hadde fått tilført mindre personell fra kommunene enn de hadde trengt og de har derfor også rekruttert personell eksternt. Like fullt har samlokaliseringen ført til at det ikke lenger er noen i deltakerkommunene som besitter formell IKT- kompetanse, eller jobber med IKT- drift. Daglig leder i samarbeidsorganisasjonen mente at det ikke var behov for å ha IKT- personell i kommunene etter etableringen av et samlet drifts- og supportmiljø. Han sa at de som ble overført fra kommunene var teknisk personell og at de i dag jobber med drift og support i samarbeidsorganisasjonen. I samtaler med representanter fra deltakerkommunene ga tre av kommunene uttrykk for at samarbeidet uten tvil hadde bidratt til bedre informasjonssikkerhet. Rådmennene i kommune 2 og 3 trakk frem at den tekniske infrastrukturen tidligere var dårlig og at de ikke hadde fullstendig oversikt over hvem som gjorde hva og hvordan. Kommunalsjefen i kommune 4 støttet rådmannen i kommune 3 ved å hevde at opprettelse av samarbeidet hadde ført til en profesjonalisering av det som nå er kommunenes felles IKT –

[115] Ot.prp. nr. 95 (2005-2006)

avdeling. Dette har igjen ført til en tryggere og mer stabil infrastruktur. Representantene i kommune 1 var litt mer tvilende. Virksomhetslederen jeg pratet med fortalte at sikkerhet hadde fått litt mer fokus og det var færre feil knyttet til fagsystemene, men både virksomhetslederen og en rådgiver pekte på at det var blitt en større distanse mellom kommunen og samarbeidsorganisasjonen og at ansvarsforhold kanskje var litt vanskeligere å få tak på i dag, enn når IKT- avdelingen var bare ”deres”.

Ut i fra dette kan en tenke seg at den tekniske sikkerheten er blitt bedre og at hver kommunes sårbarhet er redusert. Men som jeg har vært inne på er det en utbredt oppfatning at det er i tilknytning til de organisatoriske elementene at arbeid med informasjonssikkerhet viser seg å være vanskeligst. Etter gjennomgangene i kapittel 2 og 3 synes denne antagelsen å være treffende også i dette tilfellet.

En må være klar over at arbeid med sikring av personopplysninger er sammensatt og krever både juridisk og teknisk kompetanse (se Schartum 2005:105). Ser vi tilbake til avsnitt 3.1.2 hvor jeg diskuterte sikkerhetsorganisasjonen i den enkelte kommune, så vi at en eventuell sikkerhetsorganisasjon i deltakerkommunene ville være delt i to fordi både driftsavdeling og utviklingsavdeling er en del av samarbeidsorganisasjonen og ligger i deres lokaler. Særlig det at driftsorganisasjonen - og dermed den tekniske kompetansen, ligger i samarbeidsorganisasjonen kan føre til utfordringer ved gjennomføring av sikkerhetsarbeidet i deltakerkommunene. Jeg har tidligere vist at flere representanter fra kommunene anser samarbeidsorganisasjonen som ansvarlig for ivaretakelse av informasjonssikkerheten (se avsnitt 3.1.2). Det er ikke uvanlig at IKT- avdelinger får dette ansvaret. Problemet er at lovgiver har lagt opp til at kommunenes øverste ledelse skal ta initiativ og være aktiv i informasjonssikkerhetsarbeidet. Dette oppnår man ikke ved å holde informasjonssikkerhetsspørsmål innenfor en IKT- avdeling. Et større problem for kommunene i dette caset er at IKT- avdelingen er flyttet ut av den enkelte kommune og dermed har det blitt skapt større fysisk avstand til dem som normalt skal ha tatt seg av denne type spørsmål i kommunene.

Slikt sett kan en si at det nå er viktigere enn før at kommunens ledelse engasjerer seg i arbeidet på huset. I og med at arbeid med informasjonssikkerhet krever teknologisk så vel som juridisk kompetanse blir det vesentlig å ha en god dialog med teknisk-/drifts- personell i samarbeidsorganisasjonen. Fra SLA – avtalen kan vi lese at det er samarbeidsorganisasjonen

selv som plukker ut driftsansvarlige til de aktuelle fagsystemene. I avsnitt 2.9.4 så vi at SLA – avtalen gir den driftsansvarlige ansvar for å sikre at ”den tekniske driften av systemet er i henhold til gjeldende lovverk og retningslinjer for IT-sikkerhet”. Av denne formuleringen må vi forstå at de driftsansvarlige er ansvarlige for de teknologiske aspektene ved informasjonssikkerhetsarbeidet.

Eksempler på hvilke oppgaver samarbeidsorganisasjonen kan bistå med er utarbeidelse av tekniske vurderinger og spesifikasjoner vedrørende beregning av akseptabel risiko samt tekniske elementer av risikovurderinger, avvikshåndtering og revisjoner.

Per i dag ser det ikke ut til å være noen særlig utbredt dialog mellom deltakerkommunene og samarbeidsorganisasjonen vedrørende gjennomføringen av rettslige krav til informasjonssikkerhetsarbeidet. Dette virker hemmende på arbeidet.

Det er ganske tydelig at samarbeidsorganisasjonen må bidra når ivaretakelse av informasjonssikkerhet i stor grad krever teknologiske vurderinger. Likevel er det viktig å understreke at det er kommunene selv som er rettslig ansvarlig og at de ikke, etter loven, kan skyve bort sitt eget ansvar over på samarbeidsorganisasjonen slik det gjøres i dag.

## 4.2 Samarbeidsorganisasjonen - en ”myndighet uten myndighet”

Innledningsvis i kapittel 2 viste jeg til at det har blitt utarbeidet en felles veileder for internkontroll og informasjonssikkerhet og at denne inneholder spesifikasjoner vedrørende roller i tillegg til at den innholder veiledende materiell angående de gjennomførende oppgaver knyttet til informasjonssikkerhetsarbeid. Et av funnene som kom tydelig frem i kapittel 3 var likevel at det i praksis var uklart hvem som faktisk skulle gjennomføre de ulike oppgavene, eller snarere at oppgavene i praksis ikke ble gjennomført. Oppgavene som er tildelt de ulike rollene gjennom SLA- avtalen og den felles veilederen er ikke forenelig med praksis. Flere av dem jeg intervjuet i kommunene mente at informasjonssikkerhet var noe samarbeidsorganisasjonen skulle ta seg av. Den eneste kommunen som fullt og helt så på informasjonssikkerhet som sitt eget ansvar var kommune 4. Representanten fra kommune 4 understreket likevel at samarbeidsorganisasjonen var et viktig bidrag til forbedringen av den tekniske informasjonssikkerheten.

Spørsmålet om hvem som har ansvar for hva ser ut til å være vanskeligere å fastslå i praksis enn det er på papiret. Samarbeidsorganisasjonen peker på at ansvar vedrørende sikring av personopplysninger ligger hos den enkelte kommune og at de selv ikke har ansvar for at den

enkelte kommune etterlever regelverket. I presentasjonen og diskusjonen omkring begrepet behandlingsansvarlig slo jeg fast at det rettslige ansvaret for ivaretakelse av informasjonssikkerhetsbestemmelsene i pol og pof ligger til hver enkelt kommune ved deres rådmenn som behandlingsansvarlige (avsnitt 2.2 flg.).

En av kjerneoppgavene til samarbeidsorganisasjonen er å utføre driftsoppgaver for deltakerkommunene, men organisasjonen bidrar også med veiledning og råd. I begge tilfeller blir samarbeidsorganisasjonen å betrakte som et saksforberedende organ og har ingen formell beslutningsmyndighet. Beslutningsmyndigheten ligger som vi har sett hos den enkelte kommune og det er de selv som må avgjøre om de velger å ta råd og anbefalinger fra samarbeidsorganisasjonen til følge.

En rådgiver i samarbeidsorganisasjonen forklarte at de (samarbeidsorganisasjonen) var en ”myndighet uten myndighet”. I et eksempel for å utdype dette utsagnet pekte han på den felles veilederen. Samarbeidsorganisasjonen fikk i oppgave å utforme denne veilederen, men når det kom til rådgivning og forsøk på å få kommunene til implementere denne veilederen ble det raskt klart at de ikke kunne pålegge ”noen noe som helst”. Snarere kunne det oppleves som upopulært å komme med ”purringer” på kommunene for manglende implementering av retningslinjene.

Han fortalte videre at helt siden samarbeidet ble opprettet hadde ingen av kommunene, etter hans oppfatning, jobbet særlig med informasjonssikkerhet på egenhånd. Dette arbeidet var det i hovedsak samarbeidsorganisasjonen som hadde stått for. Han begrunnet dette med at det er de som har kompetansen. Etter hans oppfatning er det vanlig at IKT- avdelinger får ansvar for ivaretakelse av informasjonssikkerhet og at det også er slike tendenser i forholdet mellom deltakerkommunene og samarbeidsorganisasjonen.

Samarbeidsorganisasjonen har altså ingen myndighet ovenfor kommunen. Det er den enkelte kommune som selv har beslutningsmyndighet i forhold til arbeidet med sikring av personopplysninger i sin egen kommune. Med denne myndigheten følger et ansvar for å utøve denne på en forsvarlig måte. Dette betyr at de ikke kan overlate hele ansvaret til samarbeidsorganisasjonen, men de står selvfølgelig fritt til å be om råd og assistanse. Tilsynelatende spiller samarbeidsorganisasjonen en viktig rolle i form av utredninger, rådgivning og som pådriver for et bedre arbeid med sikkerheten. Problemene har vist seg å oppstå når rådene og veiledningsmateriell skal implementeres.

I kapittel 3 så vi at veiledningsmaterialet la opp til etablering av sikkerhetsorganisasjon og utnevnelse av sikkerhetsansvarlig (avsnitt 3.1.2). Ingen av kommunene kunne vise til at disse tiltakene var blitt gjennomført. Samme gjelder for utarbeidelse av sikkerhetsmål og strategier (avsnitt 3.1.1), arbeid med gjennomføring av risikovurderinger (avsnitt 3.2.2) og gjennomføring av sikkerhetsrevisjoner og avvikshåndtering (avsnitt 3.3.1). Ut i fra disse funnene kan det virke som om kommunene i praksis ikke gjør sin del av arbeidet. Når en ber om råd – som har blitt levert gjennom felles veiledningsmateriell, så bør en også ta i mot disse rådene og iverksette nødvendige tiltak. Uten myndighet kan heller ikke samarbeidsorganisasjonen gå inn i den enkelte kommune å gjennomføre disse tiltakene.

Tilsynelatende betrakter flere av kommunene informasjonssikkerhet som et teknologisk arbeid og ser ut til å glemme at det er kommunen selv som må stå for mange av de gjennomførende tiltakene, herunder utarbeidelse av sikkerhetsmål, strategier og utarbeide grunnlag for vurdering av akseptabel risiko, risikovurderinger, avvikshåndtering og revisjon. Som jeg var inne på over er det rimelig klart at samarbeidsorganisasjonen med sin tekniske kompetanse må bidra i forhold til teknisk relaterte vurderinger, men kommunene må selv være med på utarbeidelse av planverk og holdningsskapende arbeid i egen kommune.

Av dette kan det virke som om deltakerkommunene for lett legger oppgaver knyttet til informasjonssikkerhet til samarbeidsorganisasjonen (fordi det er her ”kompetansen” ligger), men er i mindre grad villig til å ta innover seg de anbefalinger og pålegg samarbeidsorganisasjonen legger frem.

## 4.3 Behov for forankringspunkt og bedret dialog i tilgjengelige fora

Roller knyttet til arbeid med informasjonssikkerhet er definerte. De mest sentrale rollene er definert i SLA- avtalen. Beskrivelsen av disse rollene er gjengitt og utvidet i den felles veilederen. I kommunene var alle kjent med at det var rådmennene som hadde det øverste ansvaret for kommunens plikter som behandlingsansvarlig. De var også godt inneforstått med at rollene som systemeier – tilsvarer rollen som daglig ansvarlig, og rollen som systemansvarlig. I tillegg visste alle systemeiere og systemansvarlige hvem som var driftsansvarlig- hos samarbeidsorganisasjonen, for det fagsystemet de jobbet med.

Både SLA- avtalen og den felles veilederen lister oppgaver og plikter for den enkelte rolle. I praksis synes dette likevel ikke å være helt klart.

Det kan synes som om det har oppstått et tomrom når det kommer til gjennomføring av informasjonssikkerhetsarbeidet fordi selv om roller og ansvar er tildelt på papiret, er det ikke like opplagt hvem som skal gjennomføre hvilke oppgaver.

Et tiltak kan være å opprette et koordinerende ledd eller et forankringspunkt i kommunene. Noen fra kommunen som opprettholder kontakt med samarbeidsorganisasjonen og noen som kan påse at den enkelte kommune gjennomfører sine plikter i henhold til lov og forskrift.

Det er her utnevnelse av sikkerhetsansvarlig i hver kommune kommer inn. Det å ha en person i hver av deltakerkommunene med informasjonssikkerhet som konkret definert arbeidsoppgave kan skape den koordinasjon og samordning som ser ut til å mangle i leddet mellom kommunene og samarbeidsorganisasjonen.

Etableringen av samarbeidet har ført til at det har oppstått gode forum for samarbeid på flere nivåer. Eksempelvis er organisasjonens styre satt sammen av rådmenn eller rådmannens stedfortreder. Selv om deres oppgaver i utgangspunket er av administrativ karakter, så kan det også være et forum for utveksling av ideer og tanker omkring informasjonssikkerhet. Det er forståelig at rådmennene kanskje ikke har så mye tid til dette emnet, men det er viktig med en bevisstgjøring av at det er de som har det faktiske ansvaret og at de har mye å tjene på å sette fokus på sikring av personopplysninger i egen kommune.

Ved siden av styret finnes et arbeidsutvalg. Dette er satt sammen av representanter fra alle deltakerkommunene. Ved siste samtale med en rådgiver i samarbeidsorganisasjonen fortalte han at dette arbeidsutvalget nå skulle gå igjennom den felles veilederen for informasjonssikkerhet og internkontroll, med den hensikt å revidere den og i større grad forsøke å implementere retningslinjene i deltakerkommunene. Opprettelsen av det interkommunale IKT- samarbeidet har lagt til rette for samarbeid. Samarbeid om informasjonssikkerhet er helt klart gunstig fordi kommunene i stor utstrekning har felles IKT – infrastruktur og bruker mange av de samme fagsystemene. Dermed har de mye å vinne/spare på å evaluere sikkerheten sammen. Systemeiere innenfor samme sektor i deltakerkommunene kan eksempelvis samarbeide om gjennomføring av risikovurderinger når de alle kjører på samme fagsystem og dermed står foran et temmelig likt risikonivå. Her kan de også lett involvere de driftsansvarlige i og med at samme fagsystem har samme driftsansvarlig uavhengig av hvilken kommune det driftes for.

Dersom det opprettes en sikkerhetsansvarlig i hver kommune, kan disse også vinne på å samarbeide. Tranvik har pekt på at selv om man oppretter sikkerhetsansvarlig, så får de ikke alltid gjennomført sitt arbeid i den grad som er ønskelig. Dette begrunnes i at stillingsbrøkene er små og at den kommunale ressursbruken neppe stod i forhold til arbeidsmengden til en sikkerhetsansvarlig (Tranvik i Yulex 2009:99). Dette er ikke nødvendigvis tilfellet for alle virksomheter, men på spørsmål om størrelsen på stillingsbrøken til en eventuell sikkerhetsansvarlig i deltakerkommunene, var det ingen av kommunene som mente at den ville utgjøre en full stilling. Ved at de planlagte sikkerhetsansvarlige i hver kommune samarbeider kan en muligens utøve et sterkere og kollektivt press ovenfor ledelsen og man kan avlaste individuell arbeidsmengde ved å jobbe sammen på tvers av kommunene og opp mot samarbeidsorganisasjonen.

# 5 Oppsummeringer, utfordringer og muligheter

I denne oppgaven har jeg sett på hvorvidt inngåelse av interkommunalt IKT- samarbeid påvirker deltakerkommunenes arbeid med sikring av personopplysninger. En kan si det slik at de opprinnelige utfordringene kommunene sto ovenfor i forbindelse med informasjonssikkerhet har blitt endret. Det har gått fra å være problemer knyttet til skjør og manglende teknisk infrastruktur – særlig hos de små kommunene, til større diskusjoner om fordeling av ansvar og oppgaver.

Oppgaven er gjennomført som en case- studie. Jeg har sett på et interkommunalt IKT-samarbeid bestående av fire kommuner. I og med at jeg bare har sett på ett samarbeid og at det finnes mange mulige måter å organisere interkommunale samarbeid på, kan det være vanskelig å generalisere funnene. Jeg er likevel av den oppfatning at noen av mine funn kan betegnes som interessante for flere interkommunale samarbeid og personer som jobber med og i interkommunale samarbeid. For eksempel gjelder dette funnet om utfordringer knyttet fastsetting av ansvar og myndighet og funn knyttet til rolle- og oppgavefordeling.

Utgangspunktet mitt var som nevnt å finne ut hvorvidt inngåelse av et interkommunalt IKT-samarbeid kunne påvirke deltakerkommunenes arbeid med informasjonssikkerhet. For å finne ut av dette startet jeg med å kartlegge hvordan de rettslige ansvarsforholdene etter pol og pof var fordelt mellom kommunene og samarbeidet. Her fant jeg fort ut at samarbeidsorganisasjonen i dette tilfellet ikke kunne betegnes som databehandler overfor kommunene, men at de likevel måtte ha oppgaver knyttet til ivaretakelse av sikkerheten. Alle kommunene var kjent med at de selv var behandlingsansvarlige og de hadde alle definert IKT- spørsmål som et administrativt anliggende og utpekt rådmannen som daglig leder for den behandlingsansvarliges virksomhet. I samråd med samarbeidsorganisasjonen hadde alle kommunene definert systemeiere og systemansvarlige for de ulike fagsystemene. Systemeierne tilsvarer rollen som daglig ansvarlig. Videre hadde samarbeidsorganisasjonen definert driftsansvarlig for alle fagsystemene, det er disse som har det tekniske ansvaret for fagsystemene, herunder drift og vedlikehold. De driftsansvarlige er plassert i lokalene til samarbeidsorganisasjonen og ikke i den enkelte kommune.

Videre fant jeg to roller som ikke fantes i kommunene. Dette var rollene sikkerhetsansvarlig og sikkerhetsrevisor. Det å ikke ha sikkerhetsrevisor kan forklares med at kommunene (utenom kommune 1) er små og at de ikke har ressurser til å ha en egen stilling knyttet til

sikkerhetsrevisjon. I tillegg har systemeierne fått noen revisjonsoppgaver. At det ikke finnes sikkerhetsansvarlige i kommunene er litt mer prekært enn mangelen på sikkerhetsrevisorer. Hadde kommunene hatt sikkerhetsansvarlige på plass kunne nok gjennomføringen av sikkerhetsarbeidet fått et mer systematisk preg, og mangelen på denne type personell ble tydelig når jeg begynte å se på de gjennomførende oppgavene knyttet til sikring av personopplysninger.

Etter jeg hadde sett på rolle- og ansvarsfordeling etter lov og hvordan samarbeidet og kommunene hadde definert disse, forsøkte jeg å kartlegge i hvilken grad den dokumenterte ansvars- og myndighetsfordelingen ble ivaretatt i praksis. Med dette spørsmålet ønsket jeg å finne ut hvilke oppgaver som var tillagt de ulike aktørene/ rollene og hvorvidt disse var i tråd med loven. Dette ville også fortelle meg hvordan oppgaver var delt mellom deltakerkommunene og samarbeidsorganisasjonen. Det ble tidlig klart at mange av oppgavene som er pålagt den enkelte rolle ikke ble gjennomført. Herunder utforming av sikkerhetsmål/strategi, risikovurderinger og avvikshåndtering. Dette er i seg selv et viktig funn. Ingen av kommunene kunne vise til et strukturert regime for gjennomføring av disse lovpålagte rutinene. To av kommunene har tidligere hatt besøk av Datatilsynet som den gang hadde påpekt mange avvik hos de to kommunene. Selv om disse avvikene tilsynelatende ble rettet etter kontrollene, skapte ikke tilsynsbesøkene noen ringvirkninger med hensyn til en helhetlig og kontinuerlig prosess om informasjonssikkerhetsarbeid. Med tanke på problemstillingen er det også interessant å se hvorfor det er slik, hvorfor blir ikke disse tiltakene gjennomført? Med dette kommer jeg frem til et av de mest fremtredende funnene i oppgaven. Inngåelse av det interkommunale samarbeidet har påvirket den enkelte kommunes arbeid med informasjonssikkerhet i den forstand at ansvarsforholdene i praksis har blitt uklare og at samarbeidsorganisasjonen i stor grad har blitt utpekt som ansvarlig for arbeid med informasjonssikkerhet på vegne av alle kommunene.

Ut i fra dette kan en si at det har oppstått en ansvarsfragmentering. Dynamikken mellom deltakerkommunene og samarbeidsorganisasjonen bærer preg av å være en skyld- og ansvarsdebatt. Kanskje det største problemet i dette henseende er at kommunene og samarbeidsorganisasjonen mangler et felles forankringspunkt. De som normalt ville fungert som et forankringspunkt i kommunene, de IT-ansvarlige og ildsjelene, sitter pr i dag i samarbeidsorganisasjonen og er frustrert over at deltakerkommunene ikke tar ansvar. Ved etablering av sikkerhetsansvarlige i deltakerkommunene kunne man kanskje fått et slikt

forankringspunkt. Deltakerkommunene skjøter heller ikke sine plikter som behandlingsansvarlig fullt ut, men har overlevert flere av sine oppgaver til samarbeidsorganisasjonen, som i sin tur er feilaktig definert som databehandler etter pol § 2, nr. 5.

Samarbeidsorganisasjonen ser ut til å ha blitt en slags hvilepute for kommunene. Den mest populære begrunnelsen for dette var at det er samarbeidsorganisasjonen som besitter kompetansen. Informasjonssikkerhet blir sett på som et teknisk anliggende og når all IKT-kompetanse har blitt konsentrert i samarbeidsorganisasjonen, så er det bare naturlig at de er de som hanskes med disse spørsmålene. Annen litteratur jeg har vist til peker også på at IKT-avdelinger ofte får ansvar for informasjonssikkerhetsspørsmål og at man må jobbe mer med å forankre informasjonssikkerhet hos den øverste ledelsen, slik lovgiver har lagt opp til. Når kommunenes (felles) IKT- avdeling i tillegg er flyttet ut av den enkelte kommune oppstår det en større fysisk avstand mellom kommunene og deres IKT- avdeling.

Til tross for mine funn av manglende ivaretakelse av pol og pof sine regler vil jeg ikke avskrive interkommunalt IKT- samarbeid som en god løsning for kommuners ivaretakelse av informasjonssikkerhetsarbeid. Samarbeidsorganisasjonen som har blitt studert her har på mange måter lagt til rette for god samhandling mellom kommunene om informasjonssikkerhet. For det første har utarbeidelsen av felles retningslinjer for internkontroll og informasjonssikkerhet lagt et godt grunnlag for rolle- og oppgavefordeling. Vi har sett at veilederen kan utbedres, men den danner et godt utgangspunkt. Det at veilederen skal være felles viser og at en ønsker samarbeid. For det andre har det blitt opprettet ulike fora som muliggjør samarbeid mellom kommunene med hensyn til informasjonssikkerhet. Samarbeidsorganisasjonens styre består av representanter fra alle kommunene, det er lagt opp til faglige samarbeidsgrupper og arbeidsutvalg. Dette gjør at mulighetene for styrket samarbeid og samling av kompetanse er til stede. Problemet per i dag er at de ikke blir benyttet. Hovedproblemet ser ut til å være at ledelsen i den enkelte kommune ikke viser nok interesse for de utfordringene en står ovenfor med tanke på informasjonssikkerhet og heller ikke de mulighetene samarbeid tilbyr som løsning.

Tanken var at profesjonalisering og økte midler ville bidra til en bedre sikkerhet. Utsagnene fra respondentene var tydelige når de sa at den tekniske sikkerheten hadde blitt bedre som en følge av samarbeidet. Teknisk sikkerhet har ikke vært noe jeg har gått inn for å undersøke, så

her kan jeg bare ta respondentene på ordet. Med det sagt, så kunne det vært interessant å se om dette faktisk stemte, eller om det kun er en antagelse fra kommunenes side siden den felles IKT- avdeling har oppnådd høy grad av profesjonalisering.

På bakgrunn av de analyser som er gjort i denne oppgaven ser det uansett ut til at de største utfordringene for kommunene nå er av en organisatorisk karakter.

I avsnitt 1.1 så vi at Datatilsynet anbefalte interkommunalt samarbeid om IKT fordi dette ville gi særlig de mindre kommunene et løft med hensyn til etablering av en bedre teknisk infrastruktur og at dette vil tjene informasjonssikkerheten. Gjennom studier av dette caset har vi sett at de tekniske utfordringene for deltakerkommunene etter alt å dømme er forminsket. Men desto viktigere har vi sett at nye og muligens uforutsette utfordringer har oppstått. For mye av deltakerkommunenes oppgaver har blitt ”outsourcet” og vi har fått en fragmentering av ansvar som gjør at det praktiske arbeidet med informasjonssikkerhet ikke tilfredsstiller lovens formelle krav.

På bakgrunn av funnene i denne oppgaven kan en og spørre seg om lovgiver, forskriftsmyndighet, Datatilsynet og interesseorganisasjoner som KS og KINS kan bidra med avklaringer og hjelp.

At det oppstår usikkerhet knyttet til roller, ansvar og gjennomførende oppgaver er uheldig. En kan spørre seg om lovgiver og forskriftsmyndighet har vurdert begrepsbruken sin opp mot mer dagligdagse termer. Ut i fra caset her har vi sett at man i kommunene var bedre kjent med begreper som systemeier og systemansvarlig enn *den med den daglige ledelsen og den med det daglige ansvaret*. Vi har og sett at databehandlerbegrepet er misforstått. Kanskje kan det være en idé å se på muligheter for bruk av nye begreper i lov og forskrift.

Et annet moment gjelder de lovfestede begrepers betydning. Forskriften tilbyr i liten grad definisjoner. Jeg har vist til at det kan være utfordrende å bestemme hvem som skal være behandlingsansvarlig, premisser for delt behandleransvar og hvem som skal utgjøre *den med den daglige ledelsen.* Dette er kanskje også noe som lovgiver og forskriftsmyndighet bør se på.

Vi har sett at både Datatilsynet og KS snakker varmt om inngåelse av interkommunalt samarbeid. Funnene i denne oppgaven bør dermed være en varslelampe. Dersom de vil fortsette å anbefale inngåelse av interkommunale IKT- samarbeid, bør de og være klar over at

uforutsette og organisatoriske utfordringer kan erstatte kommuners tekniske utfordringer ved etablering av et interkommunalt IKT- samarbeid.

Her kan en stille spørsmål til om Datatilsynet – kanskje i samråd med KS, bør vurdere å lage en veileder spesielt myntet på informasjonssikkerhet i interkommunale IKT- samarbeid. Her kunne man særlig tatt tak i fordeling av ansvar, roller og oppgaver mellom kommunene og samarbeidsorganisasjonen.

Selv om jeg med denne oppgaven har vist at organisering informasjonssikkerhetsarbeid gjennom interkommunale IKT- samarbeid kan være utfordrende, tror jeg at kommuner kan finne at det ligger gevinster i å samarbeide om dette. Forholdene ligger også til rette i og med at alle kommuner følger samme lovverk og nødvendigvis behandler samme type personopplysninger. I forbindelse med Rapporten "Informasjonssikkerhet i nordiske kommuner og fylkeskommuner" som nylig kom ut peker Peggy Heie i Norsis også på dette poenget. Hun sier blant annet at "*Kommuner bør samarbeide. De har samme lover og regler, og ofte samme tjenester.* "[116] Kommuner og virksomheter innenfor kommunene kan spare mye på å samarbeide om risikoanalyse, sikkerhetsledelse og eventuelle kampanjer. Jeg er likevel av den oppfatning at lovgiver, forskriftmyndigheter, Datatilsynet og folk fra fagmiljø i større grad kan bidra gjennom lovgivning og veiledning til å gjøre samarbeid om informasjonssikkerhet lettere.

[116] Intervju med Peggy Heie i Computerworld:(http://www.idg.no/computerworld/article179362.ece?curPage=2) lest 21.10.10

# Litteraturliste

***Bøker:***


Bernt, Jan Fridtjof, Hove, Harald og Overå, Oddvar (2002): Kommunalrett – 4. utgave Universitetsforlaget. Oslo.

Boe, Erik (2004): Innføring i juss – juridisk tenkning og rettskildelære. 5. opplag. Universitetsforlaget. Oslo.

Boe, Erik (2005): Grunnleggende juridisk metode – en introduksjon til rett og rettstenkning. Universitetsforlaget. Oslo.

Coll, Line og Lenth, Claude A. (2000): Personopplysningsloven – en håndbok. Kommuneforlaget: Oslo.

Daler, Torgeir et al. (2006): Håndbok i datasikkerhet – Informasjonsteknologi og risikostyring. 2. utgave. Tapir akademiske forlag. Trondheim.

Fimreite, Anne Lise og Grindheim, Jan Erik(2007): Offentlig forvaltning. 2. Utgave. Universitetsforlaget. Oslo

Grønmo, Sigmund (2004): Samfunnsvitenskaplige metoder. Fagbokforlaget Vigmostad og Bjerke AS. Bergen.

Hagen, Terje P og Sørensen, Rune J(2006) Kommunal organisering – 6. utgave. Universitetsforlaget. Oslo.

Haug, Are Vegard (2006): Rettslige reguleringer av informasjonssikkerhet. Complex nr. 2. Senter for Rettsinformatikk. Oslo

Haug, Are Vegard (2009): Lokaldemokratiet på nett og i nett. Doktoravhandling forsvart ved det samfunnsvitenskaplige fakultet, Universitetet i Oslo. No. 164

Jacobsen, Jan Ingvar(2002):Hvordan gjennomføre undersøkelser? – innføring i samfunnsvitenskaplig metode. Høyskoleforlaget AS. Kristiansand.

Johansen, Michal Wiik et al. (2001): Personopplysningsloven - Kommentarutgave. Universitetsforlaget. Oslo.

Schartum, Dag Wiese (2005): Krav til sikring av personopplysninger. Fra Arild Jansen og Dag Wiese Schartum (red.): Informasjonssikkerhet – Rettslige krav til sikker bruk av IKT. Fagbokforlaget. Bergen.

Schartum, Dag Wiese (2007): Møte mellom forvaltningsretten og personopplysningsretten. Fra Schartum, Dag Wiese (red.): Elektronisk forvaltning i Norden. Fagbokforlaget. Bergen.

Schartum, Dag Wiese og Bygrave, Lee A (2004): Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger. Fagbokforlaget. Bergen

Slay, Jill og Koronios, Andy (2006): Information Technology – Security & Risk Management. John Wiley. Sydney.

Storm, Ørnulf (2009): Organisering av informasjonssikkerhet i kommuner. Universitetet i Oslo.

Tranvik, Tommy(2009): Personvern og informasjonssikkerhet – En studie av rettsreglers etterlevelse i kommunal sektor. Complex nr. 4. Senter for Rettsinformatikk. Oslo.

Tranvik Tommy (2009): Kommuner og informasjonssikkerhet – etterlevelse av kravene i personopplysningsloven og forskriften. Fra Schartum, Dag Wiese og Bekken, Anne Gunn B. (red). Yulex 2009. Senter for rettsinformatikk/unipub. Oslo.

***Artikler:***

Aanensen, Leif T (2008): Informasjonssikkerhet – et ledelsesansvar. I Kommunenes sentralforbund (red.): IKT og ledelse. Kommuneforlaget. Oslo

Fossheim, Hallvard J.(2009): Konfidensialitet – Hentet fra www.etikkom.no (http://etikkom.no/no/FBIB/Temaer/Personvern-og-ansvar-for-den-enkelte/Konfidensialitet/) lest 13.10.2010.

Lanestedt, Gjermund(2008): IKT- Samarbeid mellom kommunene. I Kommunenes sentralforbund (red.): IKT og ledelse. Kommuneforlaget. Oslo

***Dokumenter:***

Datatilsynet - Risikovurdering av informasjonssystem. Oppdatert: 15.02.02 Opptrykk: 06.03.09

Datatilsynets årsmelding 2003

St.meld. nr. 12 (2006-2007) Regionale fortrinn – regional fremtid

Datatilsynet – En veileder om internkontroll og informasjonssikkerhet. November 2009.

Datatilsynet – Veileder: Databehandleravtaler etter personopplysningsloven og helseregisterloven. Mai 2009.

Ot.prp. nr. 95 (2005-2006) Om lov om endringar i lov 25. September 1992 nr 107 om kommuner og fylkeskommuner (interkommunalt samarbeid)

Ot.prp. nr. 92 (1998-1999) Om lov om behandling av personopplysninger (personopplysningsloven)

NOU (1997:19) Et bedre personvern – forslag til lov om behandling av personopplysninger.

Schartum, Dag Wiese og Bygrave, Lee A. (2006): Utredning av behov for endringer i personopplysningsloven. Skrevet etter oppdrag fra Justisdepartementet og Moderniseringsdepartementet.

***Standarder:***

Informasjonsteknologi: Administrasjon av informasjonssikkerhet NS-ISO/IEC 17799:2000

***Dokumentasjon fra samarbeidsorganisasjonen***

Organisasjonens vedtekter

Service Leverings Avtale (SLA)

Felles retningslinjer for internkontroll og informasjonssikkerhet

Prosjektrapport vedrørende etablering av interkommunalt IKT- samarbeid

***Muntlige kilder/Intervjuer:***

Intervju med daglig leder i samarbeidsorganisasjonen

Intervju med rådgiver i samarbeidsorganisasjonen

Intervju med virksomhetsleder i kommune 1

Intervju med rådgiver kommune 1

Intervju med rådmann kommune 2

Intervju med systemansvarlig kommune 2

Intervju med rådmann kommune 3

Intervju med beredskapsansvarlig kommune 3

Intervju med kommunalsjef kommune 4

## Figurliste



## Vedlegg

# Oversikt over vedlegg

## Intervjuguide til samtaler for å kartlegge arbeid med informasjonssikkerhet i den enkelte kommune.[1]

1. **Innledende spørsmål**
    - Hvor lenge har du jobbet i kommunen?
    - Hva går dine daglige arbeidsoppgaver ut på?
    - Har du vært involvert i arbeid relatert til inngåelse av IKT - samarbeidet?
    - Hvor mange flyttet over til IKT – samarbeidet ved etablering av IKT - samarbeidet?

2. **IKT - samarbeidet har som utgangspunkt å sørge for felles drift av fagsystemer og å drive support.**

    - Er det noen systemer dere bruker i dag som ikke driftes av IKT - samarbeidet?

        i. Er det evt. meningen at disse skal driftes av IKT - samarbeidet i fremtiden

        ii. Har dere avtaleverk med disse leverandørene som regulerer ansvar i forhold til personvern og informasjonssikkerhet?

3. **Kan du si litt om dine oppgaver i forhold til arbeid med informasjonssikkerhet i kommunen?**

4. **Hvordan vil du beskrive arbeidet med informasjonssikkerhet i kommunen?**

    - Kan du si litt om ansvarsfordeling og de enkeltes arbeidsoppgaver
        i. Systemeier og systemansvarlig?
    - Har dere en sikkerhetsorganisasjon eller lignende komité som jobber med sikkerhetsfaglige spørsmål i kommunen?
        i. Hvis ja, hvordan ser den ut, hvem er med?
        ii. Hvis ikke, er det noen enkeltpersoner som har et særskilt ansvar i forhold til sikkerhet? (det daglige ansvaret)
    - Er det noen i kommunen som har ansvaret for å gjennomføre kontroll eller revisjon knyttet til informasjonssikkerhet?

        i. Hvis ja, hvem er det og blir dette dokumentert?

5. **Vet du om dere selv har utarbeidet sikkerhetsstrategi, eller noen andre dokumenter som omhandler prioriteringer og valg knyttet til sikkerhetsarbeid?**
    - Har det blitt foretatt vurderinger av akseptabel risiko?
    - Har det blitt gjennomført risikovurderinger?
    - Hvem har i tilfellet utført dem?
    - Har dette blitt dokumentert?

[1] Benyttet som mal for intervju med Intervju med Intervju med virksomhetsleder i kommune 1, rådgiver kommune 1, systemansvarlig i kommune 2, beredskapsansvarlig kommune 3 og kommunalsjef kommune 4.

6. IKT - samarbeidet **har utformet en felles veileder for internkontroll og informasjonssikkerhet.**
    - Har dere tatt i bruk veilederen i deres kommune?
    - Hadde dere tilsvarende veildere før dere ble med i IKT - samarbeidet?

7. **Hva er etter ditt syn de viktigste utfordringene knyttet til informasjonssikkerhet i kommunen?**

8. **Etter ditt syn, har inngåelse av** IKT - samarbeidet **påvirket deres arbeid med informasjonssikkerhet?**
    - Hvordan da?
        i. Teknisk?
        ii. Organisatorisk?
    - Tror du at flytting av IT-personell til Kommune 1 og IKT – samarbeidet sine lokaler har hatt noen innvirkning på informasjonssikkerheten i deres kommune?

9. **Er det andre faktorer enn** IKT - samarbeidet **som har påvirket deres arbeid med informasjonssikkerhet?**
    - Medlemskap i KINS?
    - Veiledere fra Datatilsynet?
    - Kontroll fra Datatilsynet?
    - Noen bestemte personers innsats (ildsjeler?)

10. **Er det mulig å få kopier av eventuelle dokumenter kommunen har utarbeidet i forbindelse med IT, sikkerhet og personvern.**
    - Risikovurdering?
    - Dokumentasjon av sikkerhetsorganisasjon, sikkerhetsstrategi, sikkerhetsmål?

## Intervjuguide til samtale med rådmenn.[2]

1. **innledende spørsmål**
    - Hvor lenge har du vært rådmann i Kommunen?
    - Var du involvert i arbeidet med å etablere IKT - samarbeidet?
    - Hvor mange ansatte er det i din kommune?
    - Hvor mange flyttet over til kommune 1 ved etablering av IKT - samarbeidet?

2. **Hva vil du si er din rolle når det gjelder personverns- og informasjonssikkerhetsarbeid i din kommune, er du kjent med regelverket?**

3. **Hvordan vil du beskrive arbeidet med informasjonssikkerhet i kommunen?**
    - Hvem har det overordnede ansvaret for å sikre de opplysningene kommunen behandler?
        i. Kommunen skal ha definert kommunen v/rådmann som behandlingsansvarlig.
        ii. Hvem har den daglige ledelsen?
    - Er det etablert en sikkerhetsorganisasjon eller lignende komité som jobber med sikkerhetsfaglige spørsmål i kommunen?
        i. Hvem?
        ii. Hvis ikke, er det noen enkeltpersoner som har et særskilt ansvar i forhold til sikkerhet?
    - Er det noen i kommunen som har ansvaret for å gjennomføre kontroll eller revisjon knyttet til informasjonssikkerhet?
        i. Vet du om dette i tilfellet har blitt dokumentert?

4. **Vet du om dere selv har utarbeidet sikkerhetsstrategi, eller noen andre dokumenter som omhandler prioriteringer og valg knyttet til sikkerhetsarbeid?**
    - Har det blitt foretatt vurderinger av akseptabel risiko?
    - Har det blitt gjennomført risikovurderinger?
    - Hvem har i tilfellet utført dem?
    - Her dette blitt dokumentert?

5. IKT - samarbeidet **har utformet en felles veileder for internkontroll og informasjonssikkerhet. Den har også blitt diskutert i styret. Kan du si litt om hvem som tok initiativ til dette og i hvilken grad dere har behandlet informasjonssikkerhet i styre?**
    - Har dere tatt i bruk denne veilederen i din kommune?
    - Hadde dere tilsvarende veiledere før dere ble med i IKT - samarbeidet?

6. **Hva er etter ditt syn de viktigste utfordringene knyttet til organisering av informasjonssikkerhet i kommunen?**

[2] Benyttet til intervju med rådmennene i kommune 2 og 3.

7. **Tror du at etableringen av** IKT - samarbeidet **har påvirket deres organisering av informasjonssikkerhet samarbeid på en negativ eller positiv måte?**
    - Hvordan da?
    - Hva med at dere ikke lenger har IT-avdeling?
    - Det har skjedd en profesjonalisering, men det har skjedd sentralt, hva med lokalt?
8. **Føler du at dere har fått økt fokus på informasjonssikkerhet nå som dere er en del av IKT - samarbeidet**
    - Føler du arbeidet med informasjonssikkerhet var annerledes før i forhold til nå som dere er med i IKT – samarbeidet?
        i. På hvilken måte?
9. **(Er det noe du har spesielt lyst til å kommentere som vil ikke har vært innom)**

## Intervjuguide til samtale med daglig leder i IKT- samarbeidet.

### Innledning

Hvor mange ansatte er det i IKT – samarbeidet pr i dag?

IT-personell fra deltakerkommunene er i dag ansatt i IKT – samarbeidet via kommune 1, stemmer det?

- Er de alle fysisk plassert i kommune 1?
- Hvis ja, finnes det noen med formell IT-kompetanse igjen i de enkelte kommunene?
- Hvis nei, jobber de i full stilling med instruks fra IKT- samarbeidet?

Kan du si litt om forholdet mellom eierne og selskapet?

- Organisasjonskart (dette mulig å se?)
- Styringsmodell?
- Har det blitt lagt noen politiske føringer på hvordan samarbeidsorganisasjonen drives og deres oppgaver?
- Hva slags saker blir behandler i styremøtene, har informasjonssikkerhet noen gang vært tema på noen av styremøtene?

Opplever du at IKT – samarbeidet har tilstrekkelig med penger, personell, kompetanse til å drive i tråd med målsetningene?

### Om jobben som daglig leder

Hvilke oppgaver har du som daglig leder i IKT – samarbeidet?

Har du vært med i IKT – samarbeidet helt fra starten av?

- Hvor jobbet du før du ble daglig leder i IKT – samarbeidet?
- Hvilke forventinger hadde du til samarbeidet da det ble etablert (evt. da du startet)?

### Størrelsesforskjell på kommunene

1. Ulik grad av bidragsevne økonomisk?

### Hva var målsetningene/ambisjonene når dere satte i gang med etableringen av samarbeidet?

1. Har disse målsetningene materialisert seg?
2. Hva er de største utfordringene i et slikt samarbeid?

### Vedtekter og innlemming av kommune 4

Har det skjedd noen vedtektsendringer etter at kommune 4 ble medlem av IKT – samarbeidet?

Hentet Sak 42/08: Kommune 4 sin tilslutning til IKT – samarbeidet. Under ”premisser for tilslutning pkt 12” står det at ”Dagens ansatte i IT-avdelingen i kommune 4 får tilbud om overføring til IKT – samarbeidet i samsvar med gjeldende regelverk for virksomhetsoverdragelse og etter prosess avtalt med kommune 4.”

Kan du si litt om hvordan overdragelse av ansettelsesforhold skjer?

- Har det vært noen konflikter i forhold til overføring?
- Har alle blitt med? Noen som har sagt opp?

De gamle vedtektene sier at styre er beslutningsdyktig når Kommune 1 og en av de andre kommunene er representert, har denne vektingen blitt endret når samarbeidet har fått ett nytt medlem?

**Hensikten med etablering av IKT – samarbeidet.**

Kan du si litt om bakgrunnen for ønsket om en felles IKT- tjeneste og:

- Driftssenter i kommune 1?
- De ulike avdelingene?
- Benytter dere ekstern hjelp eller er kompetansen i IKT – samarbeidet så god at dere klarer alle oppgaver selv?
- Ved inntak av IT-personell fra deltakerkommunene, blir det gitt spesiell kursing i de systemene som skal driftes hos IKT – samarbeidet?

**Øvrige målsetninger (hentet fra forprosjekt-dokument)**

- Felles tekniske plattformer og standarder:
    - Hvordan fungerer innføring av nye felles plattformer og standarder?
    - Har dere møtt noen motstand her?

- Fellessystemer og fagsystemer:
    - Hvor mange fagsystemer er felles i dag?
        - Hvilke?
        - Er det noen som kjører helt egne systemer?
            - Hva innebærer det i tilfellet med tanke på at IKT-samarbeidet skal være en felles driftssentral?

- Kan du utdype hva som ligger i målsetningen om at utvikling skal skje i fellesskap?
    - Felles innkjøpsavtaler?
    - Er det styret som vurderer hvilke systemer som skal anskaffes i fellesskap, eller er dette mer en faglig beslutning foretatt av arbeidsutvalg, eller IT- ansatte?
    - Fungerer IKT – samarbeidet som kommunens egen IKT- avdeling?

**IKT – samarbeidet har en portefølje av programmer og tjenester:**

- Hvor mange programmer og tjenester inngår i denne porteføljen?

## Intervjuguide for første samtale med rådgiver i IKT- samarbeidet.

**Om det daglige arbeidet:**

- Hva består dine daglige arbeidsoppgaver i?
- Har du en spesiell rolle (stillingsbeskrivelse?) knyttet til informasjonssikkerhetsarbeidet som gjøres i IKT- samarbeidet og deltakerkommunene?
- Er det flere ansatte i IKT- samarbeidet med arbeidsoppgaver rettet spesifikt mot informasjonssikkerhet?
    - Teknisk?
    - Org?

**Om organiseringen**

Det har blitt utarbeidet retningslinjer for informasjonssikkerhet i IKT- samarbeidet. Slik jeg har forstått det skal disse retningslinjene gjelde for alle deltakerkommunene, stemmer det?

1. Hvis ja, ble disse retningslinjene utarbeidet i samarbeid mellom kommunene, eller er de utarbeidet sentralt hos IKT- samarbeidet?
    a. Hvilken status har dette dokumentet, har det blitt behandlet hos styret?
    b. Er det forankret lokalt hos den enkelte kommune/rådmann?
2. Hvis nei, har dere noen oversikt over om den enkelte kommunes dokumentasjon av informasjonssikkerheten (eller i hvilken grad de følger regelverket)?

I et foredrag har du vist til at kommune 1 har en intern veileder for informasjonssikkerhet fra 2001, mens du viser til varierende grad av helhetlig regelverk/dokumenterte rutiner i de andre kommunene. Kan du utdype denne uttalelsen?

1. Bruker kommune 1 fortsatt sin interne veileder eller benytter de seg av den som er utarbeidet via IKT- samarbeidet? (eller er det den gamle veilederen for kommune 1 som har blitt oppdatert og som nå skal gjelde for alle deltakerkommunene)
2. Har dere (IKT- samarbeidet) på noen måte pålagt eller oppfordret de andre deltakerkommunene til å benytte seg av veilederen dere har utformet eller bedt dem dokumentere sin sikkerhet på en bedre måte på egenhånd?
3. I forhold til relasjonen mellom dere (IKT- samarbeidet/samarbeidsorganet) og eierne (kommunene), har dere noen konkrete oppgaver knyttet til informasjonssikkerhet?

I samme foredrag betegner du IKT- samarbeidet/samarbeidsorganisasjonen som en ”Myndighet” uten myndighet, hva legger du i det?

- Hvilken myndighet er det du ønsker at samarbeidsorganisasjonen skal ha i forhold til eierne på dette området?
- Ønsket om å bruke deres kunnskap til å heve sikkerhetsnivået, men at dere mangler myndighet til å pålegge deltakerkommunene å følge et evt. regleverk?

**Om Roller og ansvar**

I utredningsdokumentet vedrørende opprettelsen av IKT - samarbeidet blir enkelte rådmann utpekt som behandlingsansvarlig og samarbeidsorganisasjonen som databehandler, stemmer dette fortsatt?

- Har du noen tanker om at samtlige rådmenn (som behandlingsansvarlige) sitter i ledelsen i databehandlerorganisasjonen(IKT - samarbeidet)?
    - Er det da i tilfellet SLA- avdelingen dere bruker som databehandleravtale?

- I forhold til loven er det kommunene v/ rådmennene som har behandleransvaret og at det er dere som databehandlere som på vegne av oppdragsgiver skal sørge for tilfredsstillende sikkerhet, hvordan føler du denne arbeidsdelingen skjer i praksis?
- Er forholdet mellom dere som databehandlerbedrift og kommunene som behandlingsansvarlige dokumentert for eksempel gjennom databehandleravtale?
- Har du oppfatning av at informasjonssikkerhet er lokalt forankret i den enkelte kommune?

Videre sies det at den med det daglige behandleransvaret varierer, med dette mener du at daglig behandleransvar er en rolle som er befestet til ulike etatsledere for ulike behandlinger?

**Avsluttende:**

Et mye brukt sitat i foredrag omkring informasjonssikkerhet er at utfordringene er 20% teknisk og 80% holdninger.

Hva mener du om det utsagnet?

1. Hva mener du er de største utfordringene i IKT - samarbeidet som helhet (inkl. deltakerkommunene)?
    a. Teknisk?
    b. Organisatorisk?
    c. Kunnskap og holdninger?

Hvordan jobber dere for å bedre disse utfordringene ?

- Holdningskampanjer?
    - Foretar samarbeidsorganisasjonen noen form for holdningsskapende virksomhet ut mot deltakerkommunene, eller er dette oppgave som hviler på deltakerkommunene selv?
- Krav?
- Kurs?
- Rundskriv?

Kan du fortelle litt om de tekniske løsningene dere har implementert med tanke på sikkerhet.

Herunder spesielt datalagring:

- Ulike soner?
- Sensitive data?
- Filservere?

Har du noen videre kommentarer til deres informasjonssikkerhetsarbeid (som vi ikke har vært innom.)

## Intervjuguide for andre samtale med rådgiver i IKT- samarbeidet

Eter SLA- avtalen skal det ha blitt utarbeidet en fullstendig oversikt som viser hvem som er utpekt til de ulike rollene både hos IKT -samarbeidet og hos kommunene. Er denne oversikten en del av kommunenes og IKT -samarbeidets felles AD?

1. Dersom det finnes en slik oversikt er det mulig å få tilgang til den?
    a. Evt. kan du si litt om hvordan den ser ut.
    b. Er den sortert etter virksomhetstype eller på kommunenivå.

Hvor mange fag og fellessystemer driftes av IKT -samarbeidet?

1. Det er oppgitt at IKT – samarbeidet drifter mellom 100 og 150 applikasjoner, hvor mange av disse betegnes som fag og fellesystemer?

Jeg har også noen spørsmål om deres arbeid med informasjonssikkerhet.

1. Har dere i IKT – samarbeidet en egen komité eller utvalg som jobber bestemt med informasjonssikkerhet og internkontroll?
2. Er det noen ansatte som har helt konkrete oppgaver knyttet til sikring av personopplysninger?
3. Har dere laget noen for strategi eller instruks som sier noe om hvem som skal gjøre hvilke oppgaver i vedrørende informasjonssikkerhet i IKT -samarbeidet?
4. Har IKT – samarbeidet gjennomført risikovurderinger i forbindlese med behandling av personopplysninger?
    a. Hvem er det evt. som har ansvar for at dette blir gjennomført?
5. Har dere i IKT – samarbeidet definert kriterier for akseptabel risiko i forhold til de systemene dere drifter for kommunene?
    a. Hvis tilfellet, hvem har gjort dette og hvem har godkjent disse
    b. Gjennomføres det revisjoner av sikkerhetsarbeidet i IKT -samarbeidet?

Jer er interessert i å vite litt mer om arbeidsoppgavene til driftsansvarlig og koordineringsansvarlig:

1. Er driftsansvarlig utpekt til å ha ansvar for et system eller kan han/henne ha driftsansvar for flere?
    a. Kan du si litt om oppgavene til en driftsansvarlig.
    b. Er det disse som tar i mot avviksmeldinger fra kommunene?
        i. Jeg antar at dette er avvik av teknisk karakter; tilgangskontroll, feilmelinger, nedetid etc.
    c. Er det et eget system på plass for å motta avviksmeldinger?
    d. Hvor ofte kommer slike meldinger inn?
    e. Finnes det felles rutiner for å ta i mot og å løse disse avvikene?

2. Kan du si litt om hvilke arbeidsoppgaver de koordineringsansvarlige har?
    a. Har de noen spesielle oppgaver knyttet til sikkerhet?
    b. Koordineringsansvarlig skal blant annet være deltaker i interkommunal faggruppe. Kan du si litt om dennes rolle i disse faggruppene. Er dette et forum hvor du ser for deg at sikkerhetsspørsmål kan bli tatt opp?

3. IKT – samarbeidet har tatt til orde for at det skal etableres sikkerhetsansvarlige i hver kommune.
    a. Betyr det at det pr i dag ikke er noen kommuner som har sikkerhetsansvarlig?
    b. Hvordan har dette ønsket blitt mottatt i den enkelte kommune?
    c. Har dere møtt forståelse for dette behovet?
    d. Når ser du for deg at en slik ordning kan være på plass?

Vi snakket tidligere om at den felles veilederen ikke var helt implementert i den enkelte kommune, ser dere noen utvikling på denne fronten?

Avslutningsvis:

Jeg har slitt litt med å forstå IKT – samarbeidet sin rolle i forhold til arbeid med informasjonssikkerhet.

Du har tidligere uttalt at IKT – samarbeidet i denne forbindelse er myndighet uten myndighet. Dere har likevel utarbeidet en felles veileder, som inneholder anvisninger på hvordan det skal jobbes med sikkerhet. Det er opp til den enkelte kommune og i verksette disse tiltakene. Av dem jeg har snakket med er det kun kommune 4 som ser ut til å ha integrert denne veilederen i sitt arbeid med informasjonssikkerhet. Hva tenker du om det? Og hva gjøres videre for å bedre dette?

Hvis jeg sier at IKT – samarbeidet i denne sammenheng blir å betrakte som et saksforberedende organ eller et rådgivningsorgan og ikke databehandler etter personopplysningsloven, hva er dine kommentarer til det?